OfficeConnect ADSL Wireless 11g Firewall Router

User Guide

3CRWE754G72-A
3CRWE754G72-B
WL-540A
WL-540B

http://www.3com.com/

Part No. DUA-0075-4AAA01

Rev. 01

Published January 2004

3Com Corporation
350 Campus Drive,
Marlborough, MA
USA 01752-3064

Copyright © 2004, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, and the 3Com logo are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

Wi-Fi and the Wi-Fi logo are registered trademarks of the WI-Fi Alliance.

IEEE and 802 are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

ABOUT THIS GUIDE

Naming Convention 7
Conventions 8
  Feedback about this User Guide 8
  Related Documentation 9

1 INTRODUCING THE ROUTER

OfficeConnect ADSL Wireless11g Firewall Router 11
Router Advantages 13
Package Contents 13
Minimum System and Component Requirements 14
Front Panel 14
Rear Panel 15

2 HARDWARE INSTALLATION

Introduction 17
  Safety Information 17
Positioning the Router 17
  Using the Rubber Feet 18
Powering Up the Router 18
Connecting the Router 18

3 SETTING UP YOUR COMPUTERS

Obtaining an IP Address Automatically 23
  Windows 2000 23
  Windows XP 25
  Windows 95/98/ME 25
  Macintosh 25
Disabling PPPoE and PPTP Client Software 26
Disabling Web Proxy 26

4 RUNNING THE SETUP WIZARD

Accessing the Wizard 27
    29
    DSL Settings 29
    Summary 33

5 ROUTER CONFIGURATION

Navigating Through the Router Configuration Pages 35
    Main Menu 35
Status Screen 35
    Status 36
LAN Setup 36
    LAN Settings 37
    DHCP Clients List 38
Wireless 39
    Configuring Wireless 39
    Encryption 40
    Disabled 41
    WPA-PSK (no server) 41
    128-bit WEP 42
    64-bit WEP 42
    WPA (with RADIUS Server) 43
Internet Settings 44
    Connection Type 44
    PPPoE 45
    PPPoA 46
    Bridged Mode for Single PC 47
    Routing Mode over ATM 47
    DNS 48
Routing 48
    Static Routes 49
    RIP Parameters 49
    Routing Table 50
Firewall 51
    Special Applications 52
    Virtual Servers 53
    Client IP Filters 54

    Access Control 54
    URL Blocking 56
    Schedule Rule 57
    MAC Address Filtering 59
    DMZ 60
    Advanced 60
SNMP 63
    SNMP Community 63
    SNMP Trap 64
System Tools 65
    Restart Router 65
    Reset to Factory Default 65
    Backup/Restore Settings 66
    Upgrade 66
    Admin Password 67
    Time and Time Zone 68
Status and Logs 69
    ADSL Status 69
    Logs 69

6 TROUBLESHOOTING

Basic Connection Checks 71
Browsing to the Router Configuration Screens 71
Connecting to the Internet 72
Forgotten Password and Reset to Factory Defaults 72
Wireless Networking 73
Recovering from Corrupted Software 74
Frequently Asked Questions 75

A IP ADDRESSING

The Internet Protocol Suite 77
Managing the Router over the Network 77
    IP Addresses and Subnet Masks 77
How does a Device Obtain an IP Address and Subnet Mask? 79
    DHCP Addressing 79
    Static Addressing 79
    Auto-IP Addressing 79

B TECHNICAL SPECIFICATIONS

OfficeConnect ADSL Wireless 11g Firewall Router 81
Standards 82

C SAFETY INFORMATION

D END USER SOFTWARE LICENSE AGREEMENT

D OBTAINING SUPPORT FOR YOUR PRODUCT

Register Your Product to Gain Service Benefits 91
Purchase Value-Added Services 91
Troubleshoot Online 91
Access Software Downloads 92
Contact Us 92
Telephone Technical Support and Repair 92

GLOSSARY

INDEX

REGULATORY NOTICES FOR THE OFFICECONNECT ADSL WIRELESS 11G FIREWALL ROUTER

ABOUT THIS GUIDE

This guide describes how to install and configure the OfficeConnect ADSL Wireless 11g Firewall Router (3CRWE754G72-A/B).

This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet Routers.

If a release note is shipped with the ADSL 11g Wireless Router and contains information that differs from the information in this guide, follow the information in the release note.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

`http://www.3com.com`

Naming Convention

Throughout this guide, the OfficeConnect ADSL Wireless 11g Firewall Router is referred to as the "Router".

Category 3 and Category 5 Twisted Pair Cables are referred to as Twisted Pair Cables throughout this guide.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
ℹ	Information note	Information that describes important features or instructions.
⚠	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
⚡	Warning	Information that alerts you to potential personal injury.

Table 2 Text Conventions

Convention	Description
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- OfficeConnect ADSL Wireless 11g Firewall Router User Guide
- Part Number DUA0075-4AAA01
- Page 24

Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to the Support and Safety Information sheet.

Related Documentation

In addition to this guide, each Router document set includes one Installation Guide. This guide contains the instructions you need to install and configure your Router.

1

INTRODUCING THE ROUTER

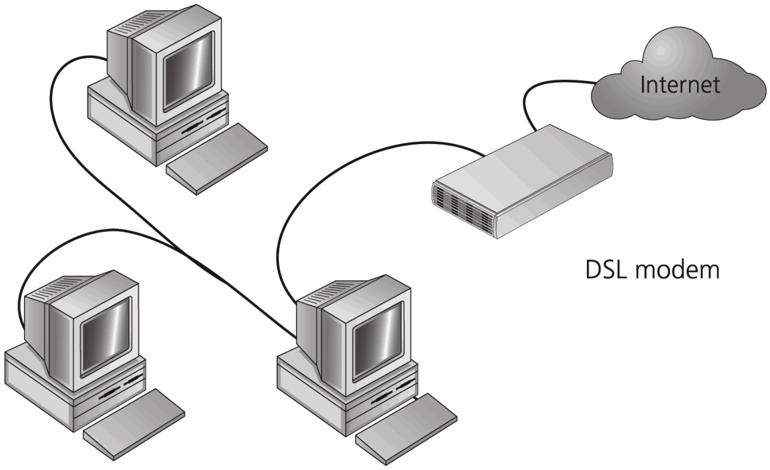
Welcome to the world of networking with 3Com®. In the modern business environment, communication and sharing information is crucial. Computer networks have proved to be one of the fastest modes of communication but, until recently, only large businesses could afford the networking advantage.

OfficeConnect ADSL Wireless11g Firewall Router

The OfficeConnect ADSL Wireless11g Firewall Router is designed to provide a cost-effective means of sharing a single broadband Internet connection amongst several wired and wireless computers. The Router also provides protection in the form of an electronic "firewall" preventing anyone outside of your network from seeing your files or damaging your computers. The Router can also prevent your users from accessing Web sites which you find unsuitable.

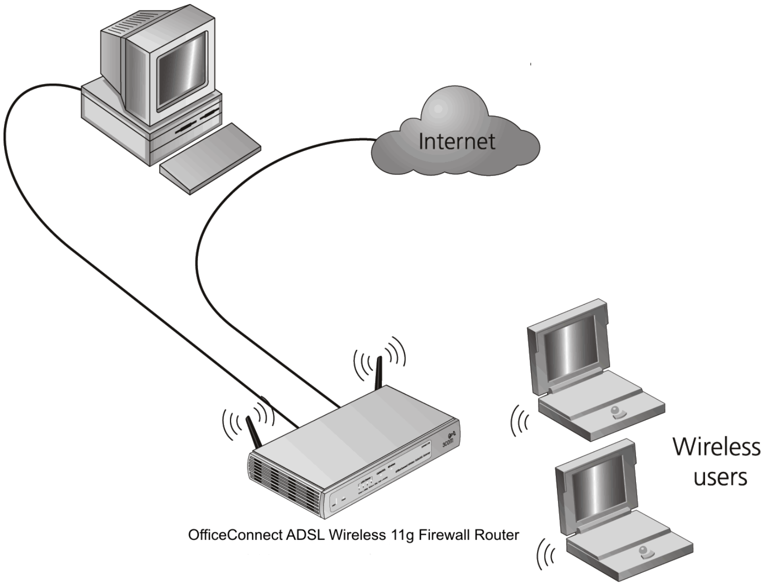
Figure 1 shows an example network without a Router. In this network, only one computer is connected to the Internet. This computer must always be powered on for the other computers on the network to access the Internet.

Figure 1 Example Network Without a Gateway


Internet
DSL modem

When you use the Router in your network (Figure 2), it becomes your connection to the Internet. Connections can be made directly to the Router, or to an OfficeConnect Switch or Hub, expanding the number of computers you can have in your network.

Figure 2 Example Network Using a Wireless DSL Router


Internet
Wireless users
OfficeConnect ADSL Wireless 11g Firewall Router

Router Advantages

The advantages of the Router include:

- Shared Internet connection for both wired and wireless computers
- High speed 802.11g wireless networking
- No need for a dedicated, "always on" computer serving as your Internet connection
- Cross-platform operation for compatibility with Windows, Unix and Macintosh computers
- Easy-to-use, Web-based setup and configuration
- Provides centralization of all network address settings (DHCP)
- Acts as a Virtual server to enable remote access to Web, FTP, and other services on your network
- Security — Firewall protection against Internet hacker attacks and encryption to protect wireless network traffic

Package Contents

The Router kit includes the following items:

- One OfficeConnect ADSL Wireless11g Firewall Router
- One power adapter for use with the Router
- Four rubber feet
- One Telephone Cable
- One CD-ROM containing this User Guide
- Installation Guide
- One Support and Safety Information Sheet
- One Warranty Flyer

If any of these items are missing or damaged, please contact your retailer.

Minimum System and Component Requirements

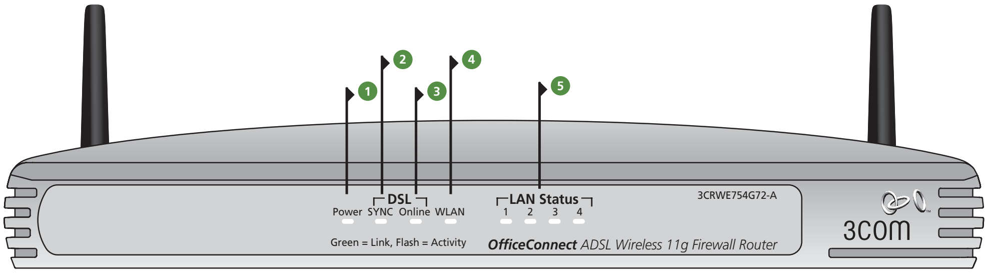
Your Router requires that the computer(s) and components in your network be configured with at least the following:

- A computer with an operating system that supports TCP/IP networking protocols (for example Windows 95/98/NT/Me/2000/XP, Unix, Mac OS 8.5 or higher).
- An Ethernet 10Mbps or 10/100 Mbps NIC for each computer to be connected to the four-port switch on your Router.
- An 802.11b or 802.11g wireless NIC.
- An active ADSL subscription and connection.
- A Web browser that supports JavaScript, such as Netscape 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher.

Front Panel

The front panel of the Router contains a series of indicator lights (LEDs) that help describe the state of various networking and connection operations.

Figure 3 Router - Front Panel


1
2
3
4
5
DSL
Power
SYNC
Online
WLAN
LAN Status
1
2
3
4
3CRWE754G72-A
Green = Link, Flash = Activity
OfficeConnect ADSL Wireless 11g Firewall Router
3com

1 Power LED

Green

Indicates that the Router is powered on.

2 DSL Sync LED

Green

If the LED is on it indicates that DSL connection is present. This LED's flashes during configuration at power up.

3 DSL Online LED

Green

If this LED illuminates successful Username/Password has been authenticated with your ISP.

4 Wireless LAN (WLAN) Status LED

Green

If the LED is on it indicates that wireless networking is enabled. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, the Wireless LAN has been disabled in the Router, or there is a problem. Refer to Chapter 6 "Troubleshooting".

5 Four LAN Status LEDs

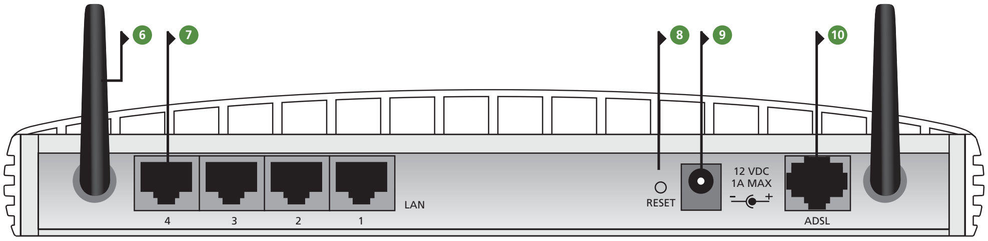
Green (100Mbps link / 10Mbps link)

If the LED is on, the link between the port and the next piece of network equipment is OK. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, nothing is connected, or the connected device is switched off, or there is a problem with the connection (refer to Chapter 6 "Troubleshooting"). The port will automatically adjust to the correct speed and duplex.

Rear Panel

The rear panel (Figure 4) of the Router contains four LAN ports, one ADSL port, a reset button, and a power adapter socket.

Figure 4 Router - Rear Panel



6 Wireless Antennae

The antennae on the product should be placed in a 'V' position when initially installed.

CAUTION: *Do not force the antennae beyond their mechanical stops. Rotating the antennae further may cause damage.*

7 Ethernet Ports

Using suitable RJ45 cables, you can connect your Router to a computer, or to any other piece of equipment that has an Ethernet connection (for example, a hub or a switch). These ports have an automatic MDI/MDIX feature, which means either straight-through or a crossover cable can be used.

8 Reset Button

If you want to reset your Router to factory default settings, and cannot access the web management interface (for example, due to a lost password), then you may use this button. Refer to "Forgotten Password and Reset to Factory Defaults" on page 72 for further details.

9 Power Adapter Socket

Only use the power adapter that is supplied with this Router. Do not use any other adapter.

10 ADSL Port

Using the RJ11 cable provided, you should connect your Router to the telephone socket via a splitter.

2

HARDWARE INSTALLATION

Introduction

This chapter will guide you through a basic installation of the Router, including:

- Connecting the Router to the Internet.
- Connecting the Router to your network.
- Setting up your computers for networking with the Router.

Safety Information

WARNING: *Please read the “Safety Information” section in Appendix C before you start.*

VORSICHT: *Bitte lesen Sie den Abschnitt “Wichtige Sicherheitshinweise” sorgfältig durch, bevor Sie das Gerät einschalten.*

AVERTISSEMENT: *Veuillez lire attentivement la section “Consignes importantes de sécurité” avant de mettre en route.*

Positioning the Router

You should place the Router in a location that:

- is conveniently located for connection to the telephone socket.
- is centrally located to the wireless computers that will connect to the Router. A suitable location might be on top of a high shelf or similar furniture to optimize wireless connections to computers in both horizontal and vertical directions, allowing wider coverage.
- allows convenient connection to the computers that will be connected to the four LAN ports on the rear panel, if desired.
- allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.

When positioning your Router, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. 3Com recommends you provide a minimum of 25 mm (1 in.) clearance.

Using the Rubber Feet

Use the four self-adhesive rubber feet to prevent your Router from moving around on your desk or when stacking with flat top units. Only stick the feet to the marked areas at each corner of the underside of your Router.

Powering Up the Router

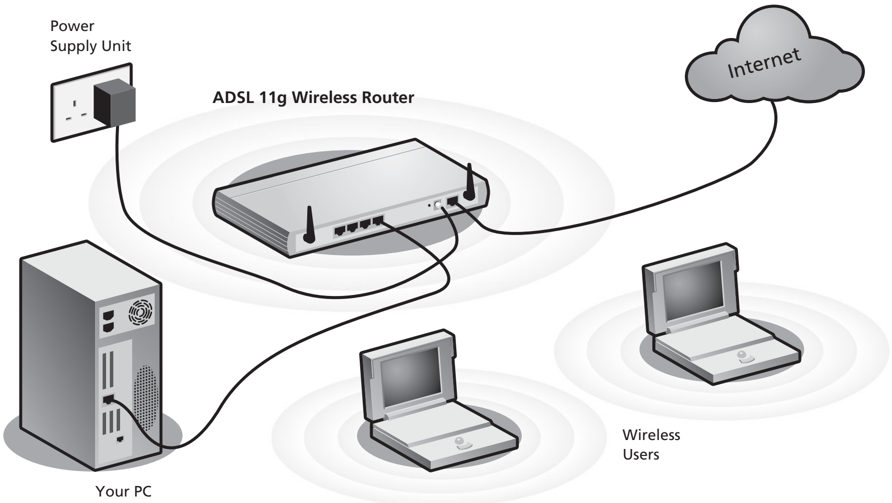
To power up the Router:

1. Plug the power adapter into the power adapter socket located on the back panel of the Router.
2. Plug the power adapter into a standard electrical wall socket.

Connecting the Router

The first step for installing your Router is to physically connect it to the telephone socket and then connect it to a computer in order to be able to access the Internet. See Figure 5:

Figure 5 Connecting the Gateway

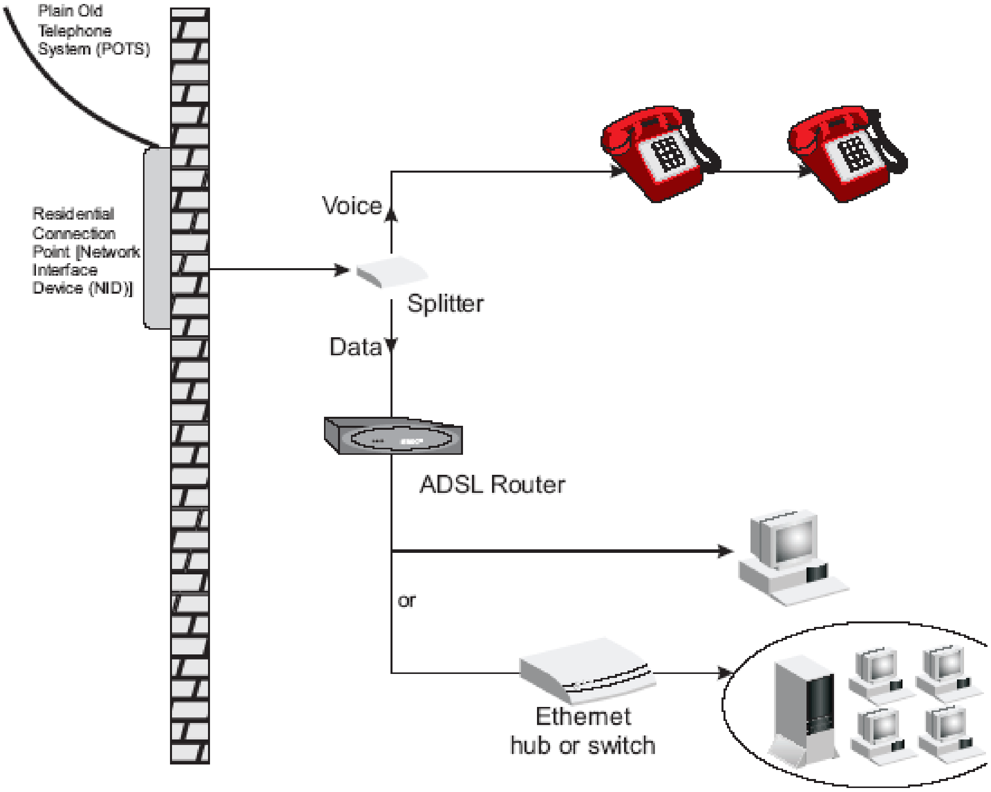


3 Run the provided telephone cable from the wall jack providing ADSL service to the ADSL port on your ADSL Router. When inserting an ADSL RJ-11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. If you are using splitterless ADSL service, add low-pass filters between the ADSL wall jack and your telephones. (These filters pass voice signals through but filter data signals out.)

Either:

If you are using a full-rate (G.dmt) connection, your service provider will attach the outside ADSL line to a data/voice splitter. In this case you can connect your phones and computer directly to the splitter as shown below (Figure 6):

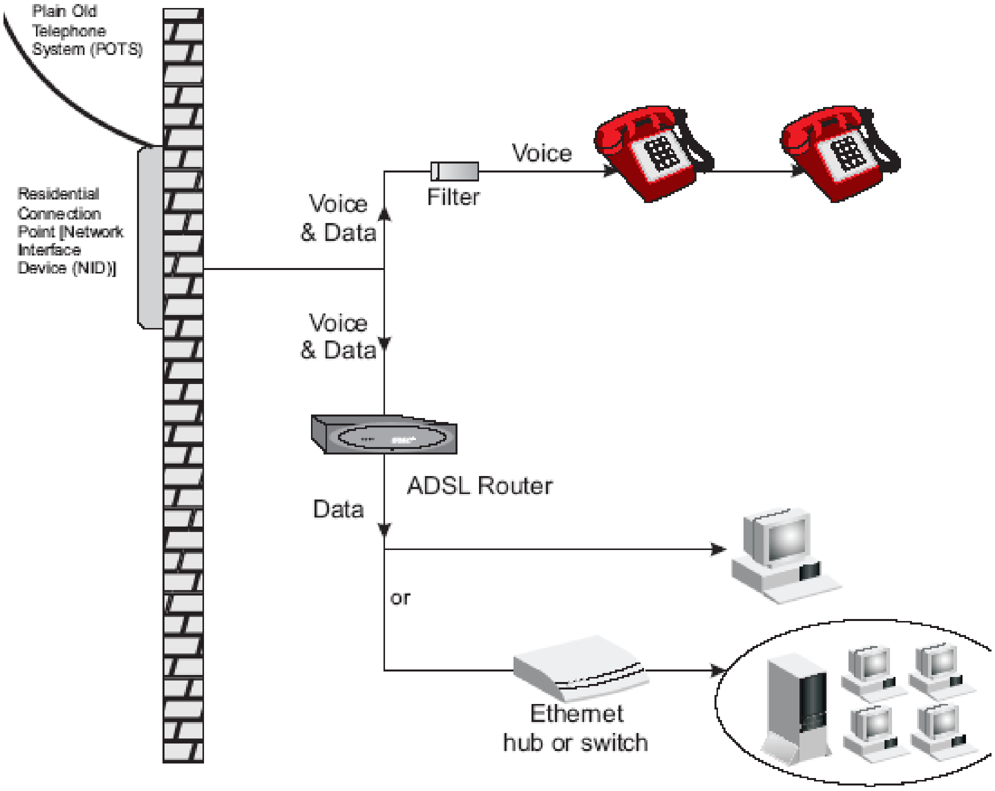
Figure 6 Installing with a splitter


Plain Old Telephone System (POTS)
Residential Connection Point [Network Interface Device (NID)]
Voice
Splitter
Data
ADSL Router
or
Ethernet hub or switch

or

If you are using a splitterless (G.lite) connection, then your service provider will attach the outside ADSL line directly to your phone system.In this case you can connect your phones and computer directly to the incoming ADSL line, but you will have to add low-pass filters to your phones as shown below (Figure 7):

Figure 7 Installing without a splitter


Plain Old
Telephone
System (POTS)
Residential
Connection
Point [Network
Interface
Device (NID)]
Voice
& Data
Filter
Voice
Voice
& Data
ADSL Router
Data
or
Ethernet
hub or switch

You have now completed the hardware installation of your Router. Next you need to set up your computers so that they can make use of the Router to communicate with the Internet.

3Com recommends that you perform the initial Router configuration from a computer that is directly connected to one of the LAN ports.

If you configure the Router from a wireless computer, note that you may lose contact with the Router if you change the wireless configuration.

To communicate wirelessly with your Router, your wireless NIC should be set as follows:

- Encryption — none
- SSID — 3Com
- Channel — 11

3 SETTING UP YOUR COMPUTERS

The Router has the ability to dynamically allocate network addresses to the computers on your network, using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter.

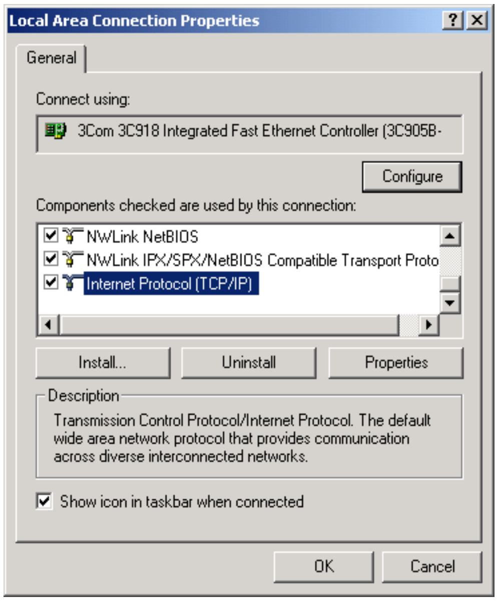
Obtaining an IP Address Automatically

Windows 2000

If you are using a Windows 2000-based computer, use the following procedure to change your TCP/IP settings:

1. From the Windows *Start* Menu, select *Settings* > *Control Panel*.
2. Double click on *Network and Dial-Up Connections*.
3. Double click on *Local Area Connection*.
4. Click on *Properties*.
5. A screen similar to Figure 8 should be displayed. Select *Internet Protocol TCP/IP* and click on *Properties*.

Figure 8 Local Area Properties Screen



Local Area Connection Properties

General

Connect using:

3Com 3C918 Integrated Fast Ethernet Controller (3C905B-

Components checked are used by this connection:

- ☑ NWLink NetBIOS
- ☑ NWLink IPX/SPX/NetBIOS Compatible Transport Proto
- ☑ Internet Protocol (TCP/IP)

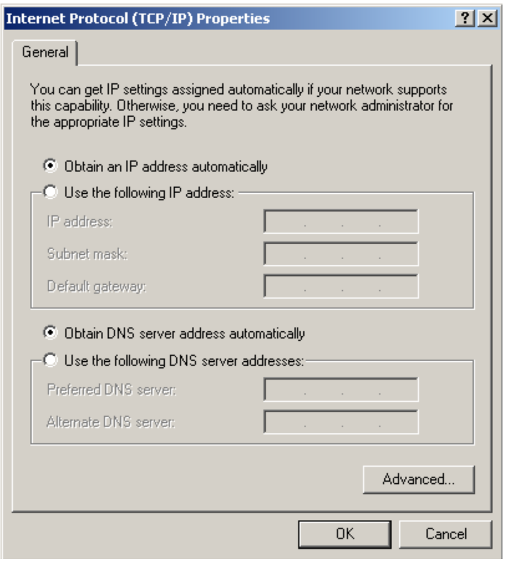
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

6 Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS server address automatically* are both selected as shown in Figure 9. Click *OK*.

Figure 9 Internet Protocol (TCP/IP) Properties Screen



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

7 Restart your computer.

Windows XP

1. From the Windows *Start* menu, select *Control Panel*.
2. Click on *Network and Internet Connections*.
3. Click on the *Network Connections* icon.
4. Double click on *LAN* or *High Speed Connection* icon. A screen titled *Local Area Connection Status* will appear.
5. Select *Internet Protocol TCP/IP* and click on *Properties*.
6. Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS servers automatically* are both selected. Click *OK*.
7. Restart your computer.

Windows 95/98/ME

1. From the Windows *Start* Menu, select *Settings* > *Control Panel*.
2. Double click on *Network*. Select the *TCP/IP* item for your network card and click on *Properties*.
3. In the TCP/IP dialog, select the *IP Address* tab, and ensure that *Obtain IP address automatically* is selected. Click *OK*.

Macintosh

If you are using a Macintosh computer, use the following procedure to change your TCP/IP settings:

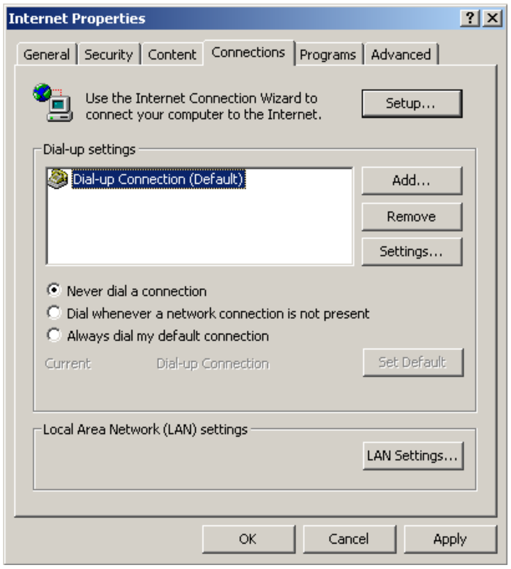
1. From the desktop, select *Apple Menu*, *Control Panels*, and *TCP/IP*.
2. In the *TCP/IP* control panel, set *Connect Via:* to “Ethernet”.
3. In the TCP/IP control panel, set *Configure:* to “Using DHCP Server.”
4. Close the *TCP/IP* dialog box, and save your changes.
5. Restart your computer.

Disabling PPPoE and PPTP Client Software

If you have PPPoE client software installed on your computer, you will need to disable it. To do this:

1. From the Windows *Start* menu, select *Settings* > *Control Panel*.
2. Double click on *Internet* Options.
3. Select the *Connections* Tab. A screen similar to Figure 10 should be displayed.
4. Select the *Never Dial a Connection* option.

Figure 10 Internet Properties Screen


Internet Properties
? ×
General
Security
Content
Connections
Programs
Advanced
Setup...
Dial-up settings
Dial-up Connection (Default)
Add...
Remove
Settings...
Set Default
Local Area Network (LAN) settings
LAN Settings...
OK
Cancel
Apply

Use the Internet Connection Wizard to connect your computer to the Internet.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current Dial-up Connection

You may wish to remove the PPPoE client software from your computer to free resources, as it is not required for use with the Router.

Disabling Web Proxy

Ensure that you do not have a web proxy enabled on your computer.

Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click *LAN Settings* at the bottom. Make sure that the *Use Proxy Server* option is unchecked.

4

RUNNING THE SETUP WIZARD

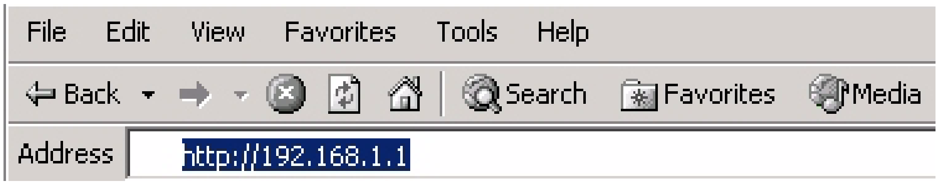
Accessing the Wizard

The Router setup program is Web-based, which means that it is accessed through your Web browser (Netscape Navigator 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher).

To use the Setup Wizard:

1. Ensure that you have at least one computer connected to the Gateway. Refer to Chapter 2 for details on how to do this.
2. Launch your Web browser on the computer.
3. Enter the following URL in the location or address field of your browser: `http://192.168.1.1` (Figure 11). The Login screen displays.

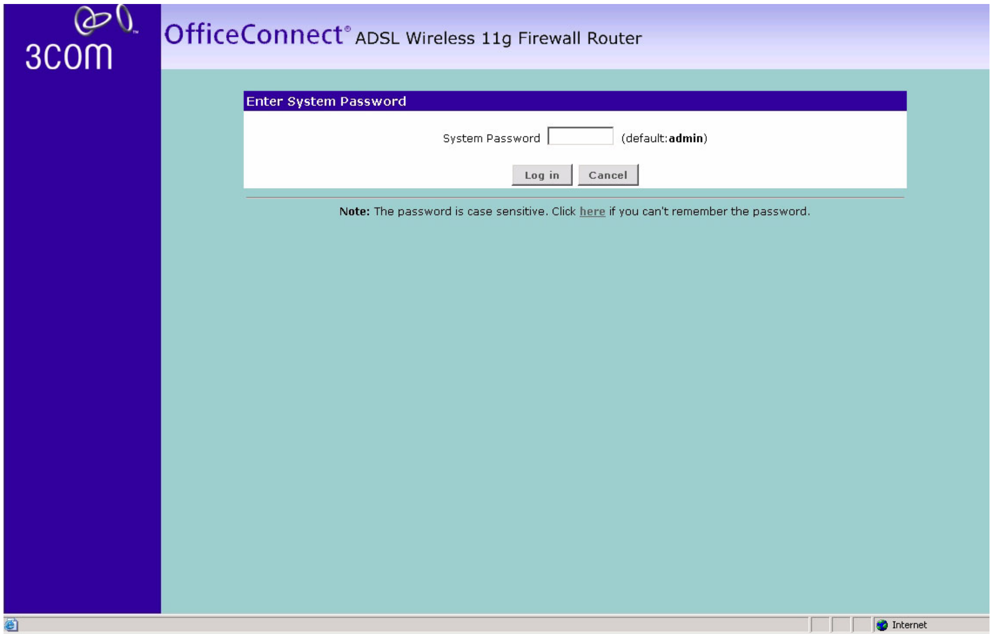
Figure 11 Web Browser Location Field (Factory Default)



Address http://192.168.1.1

4. To log in as an administrator, enter the password (the default password is *admin*) in the *Password* field and click *Log in* (Figure 12).

Figure 12 Router Login Screen



OfficeConnect® ADSL Wireless 11g Firewall Router

Enter System Password

System Password ☐ (default:**admin**)

Note: The password is case sensitive. Click here if you can't remember the password.

5 When you have logged in either:

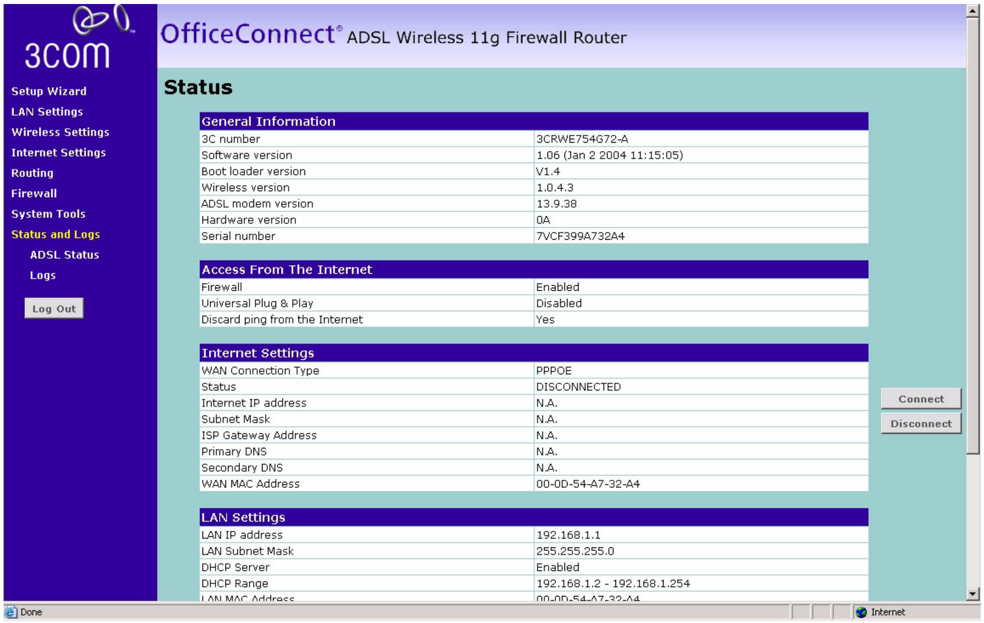
- The *Status* screen will appear (Figure 13). Select *Wizard* from the menu.

  or

- If your Router has not been configured before, the Wizard will launch automatically (refer to Figure 14).

6 You will be guided step by step through a basic setup procedure.

Figure 13 Status Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
ADSL Status
Logs
Log Out
Connect
Disconnect
Done
Internet

Status

General Information	
3C number	3CRWE754G72-A
Software version	1.06 (Jan 2 2004 11:15:05)
Boot loader version	V1.4
Wireless version	1.0.4.3
ADSL modem version	13.9.38
Hardware version	0A
Serial number	7VCF399A732A4

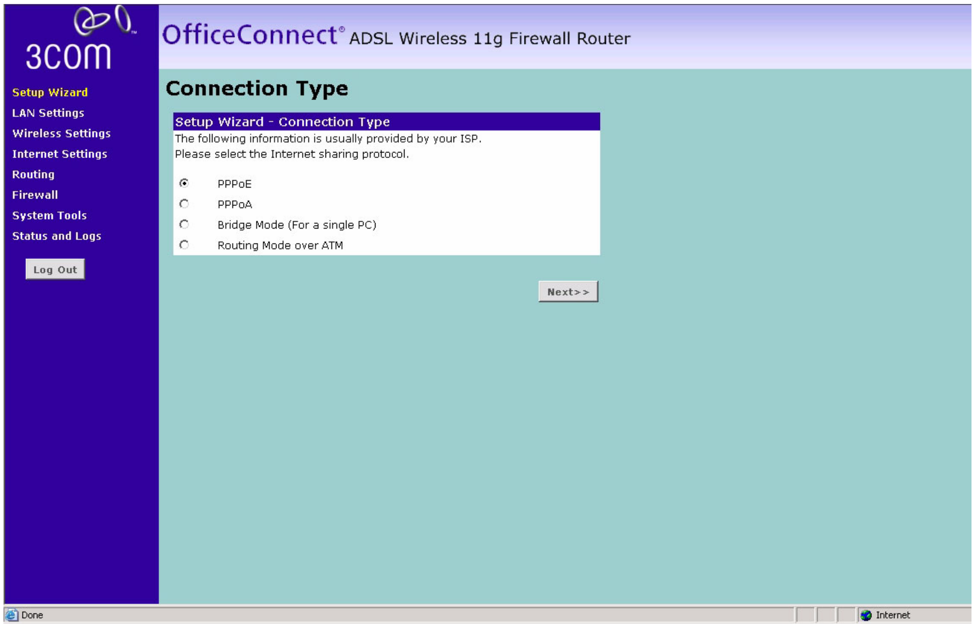
Access From The Internet	
Firewall	Enabled
Universal Plug & Play	Disabled
Discard ping from the Internet	Yes

Internet Settings	
WAN Connection Type	PPPOE
Status	DISCONNECTED
Internet IP address	N.A.
Subnet Mask	N.A.
ISP Gateway Address	N.A.
Primary DNS	N.A.
Secondary DNS	N.A.
WAN MAC Address	00-0D-54-A7-32-A4

LAN Settings	
LAN IP address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP Server	Enabled
DHCP Range	192.168.1.2 - 192.168.1.254
LAN MAC Address	00-0D-54-A7-32-A4

DSL Settings

Figure 14 DSL Settings Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Next>>
Done
Internet

Connection Type

Setup Wizard - Connection Type

The following information is usually provided by your ISP.
Please select the Internet sharing protocol.

● PPPoE
○ PPPoA
○ Bridge Mode (For a single PC)
○ Routing Mode over ATM

The *DSL Mode* window allows you to set up the Router for the type of Internet connection you have. Before setting up your DSL connection mode, have your account information from your ISP ready.

Select a DSL mode from the following:

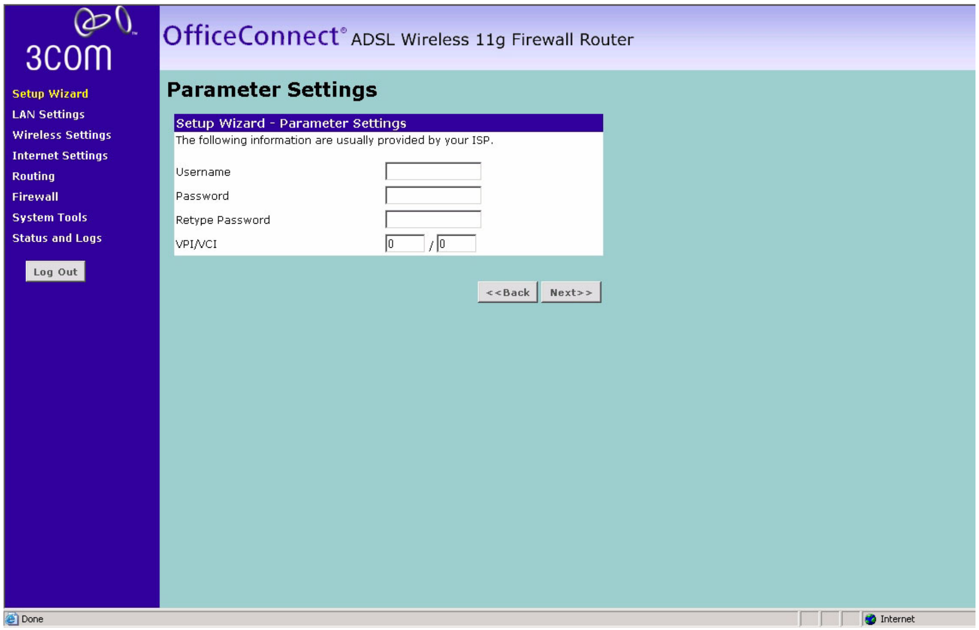
- PPPoE see page 30
- PPPoA see page 31
- RFC1483 Bridged see page 32
- RFC1483 Routed see page 31

and click *Next*.

For further information on selecting a mode see "Internet Settings" on page 44.

PPPoE Mode

Figure 15 PPPoE Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
<<Back
Next>>
Done
Internet

Parameter Settings

Setup Wizard - Parameter Settings

The following information are usually provided by your ISP.

Username

Password

Retype Password

VPI/VCI 0 / 0

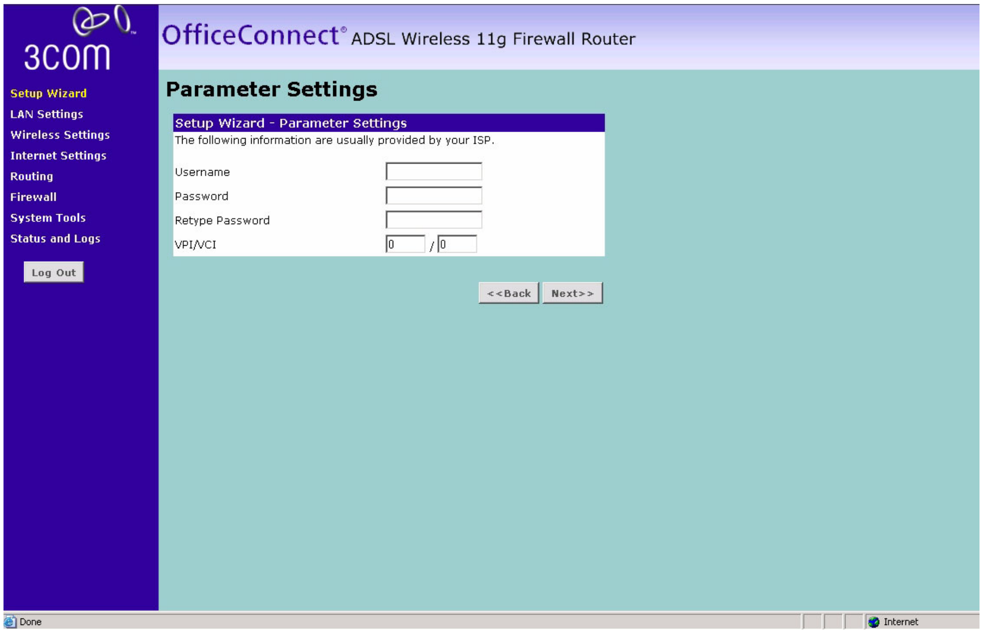
To setup the router for use with a PPP over Ethernet (PPPoE) connection, use the following procedure:

1. Enter your PPP over Ethernet user name in the *Username* text box.
2. Enter your PPP over Ethernet password in the *Password* text box.

3. Re-type your PPP over Ethernet password in the *Retype Password* text box.
4. Enter your VPI and VCI information in the *VPI/VCI* text boxes.
5. Check all of your settings, and then click *Next*.

PPPoA Mode

Figure 16 PPPoA Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
<<Back
Next>>
Done
Internet

Parameter Settings

Setup Wizard - Parameter Settings

The following information are usually provided by your ISP.

Username

Password

Retype Password

VPI/VCI 0 / 0

To setup the router for use with a PPP over ATM (PPPoA) connection, use the following procedure:

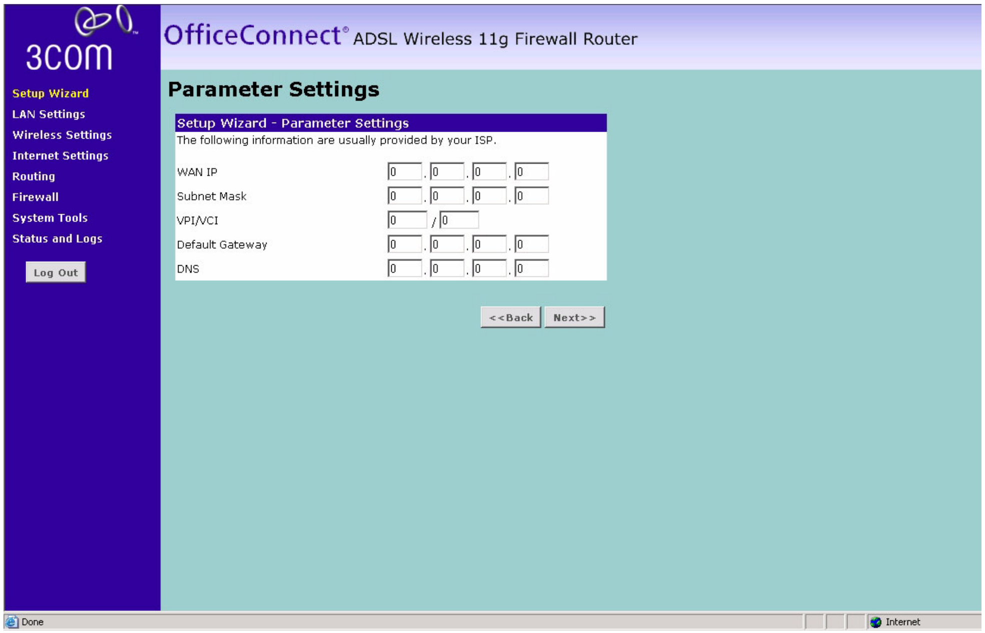
1. Enter your PPP over ATM user name in the *Username* text box.
2. Enter your PPP over ATM password in the *Password* text box.
3. Re-type your PPP over ATM password in the *Retype Password* text box.
4. Enter your VPI and VCI information in the *VPI/VCI* text boxes.

Check all of your settings, and then click *Next*.

RFC1483 Routed Mode

To setup the Router for use with an RFC1483 routed connection:

Figure 17 RFC1483 Routed Configuration Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
<<Back
Next>>
Done
Internet

Parameter Settings

Setup Wizard - Parameter Settings

The following information are usually provided by your ISP.

WAN IP 0 . 0 . 0 . 0
Subnet Mask 0 . 0 . 0 . 0
VPI/VCI 0 / 0
Default Gateway 0 . 0 . 0 . 0
DNS 0 . 0 . 0 . 0

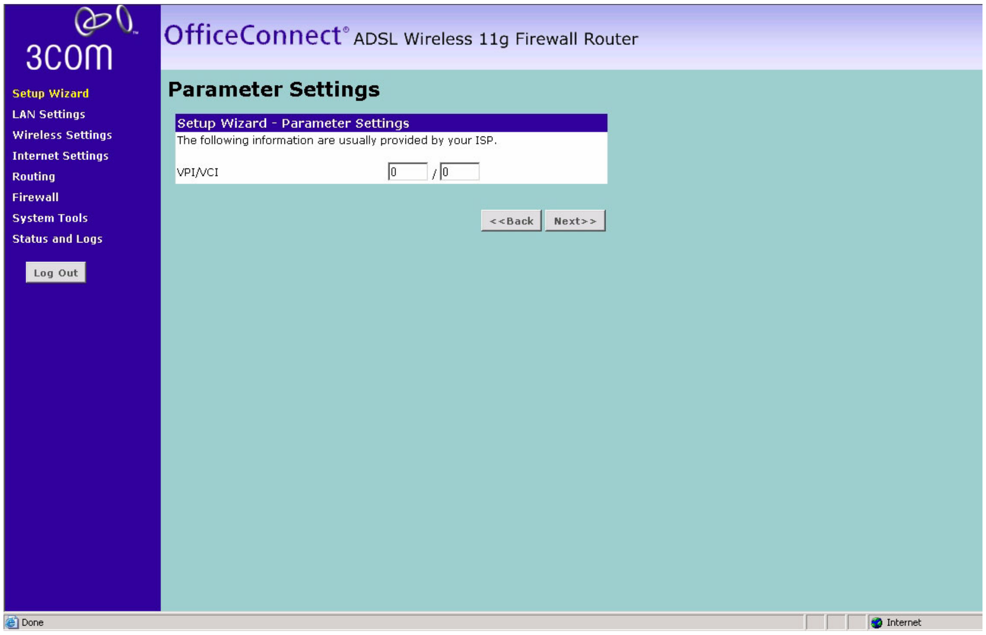
1. Enter your Internet IP address in the *WAN IP* text box.
2. Enter the subnet mask in the *Subnet Mask* text box.
3. Enter your VPI and VCI information in the *VPI/VCI* text boxes.
4. Enter the default gateway in the *Default Gateway* text box.

Check all of your settings, and then click *Next*.

RFC1483 Bridged Mode

To setup the Router for use with an RFC1483 bridged connection:

Figure 18 RFC1483 Bridged Configuration Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
<<Back
Next>>
Done
Internet

Parameter Settings

Setup Wizard - Parameter Settings

The following information are usually provided by your ISP.

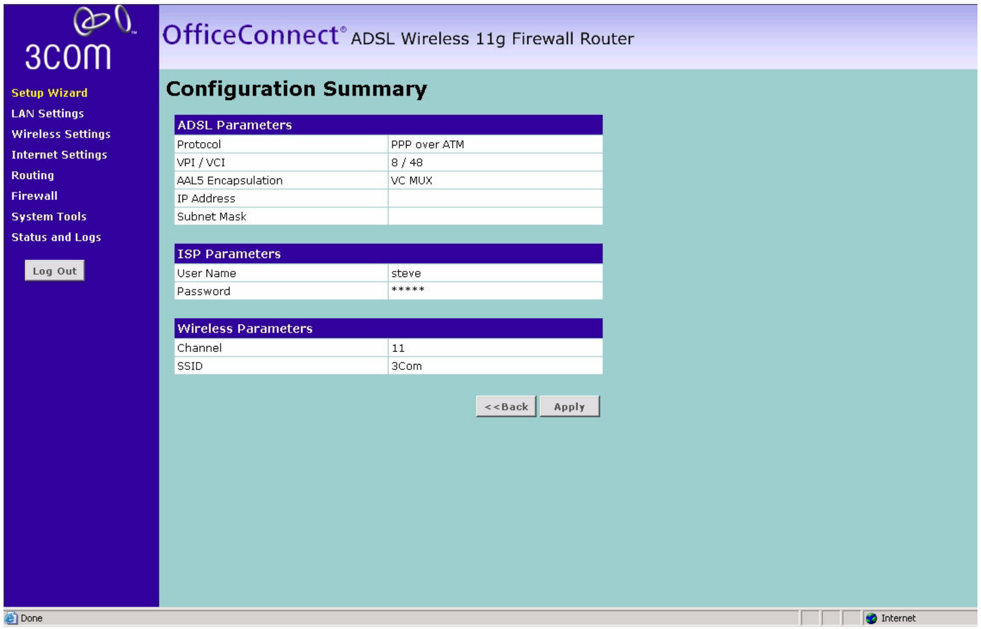
VPI/VCI 0 / 0

5 Enter your VPI and VCI information in the *VPI/VCI* text boxes.

Check all of your settings, and then click *Next*.

Summary

Figure 19 Configuration Summary Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
<<Back
Apply
Done
Internet

Configuration Summary

ADSL Parameters	
Protocol	PPP over ATM
VPI / VCI	8 / 48
AAL5 Encapsulation	VC MUX
IP Address	
Subnet Mask	

ISP Parameters	
User Name	steve
Password	*****

Wireless Parameters	
Channel	11
SSID	3Com

When you complete the Setup Wizard, a configuration summary will display. Verify the configuration information of the Router and then click *Apply* to save your settings. 3Com recommends that you print this page for your records.

Your Router is now configured and ready for use.

See Chapter 5 for a detailed description of the Router configuration screens.

5

ROUTER CONFIGURATION

Navigating Through the Router Configuration Pages

This chapter describes all the screens available through the Router configuration pages, and is provided as a reference. To get to the configuration pages, browse to the Router by entering the URL in the location bar of your browser. The default URL is `http://192.168.1.1` but if you changed the Router LAN IP address during initial configuration, use the new IP address instead. When you have browsed to the Router, log in using your system password (default password is *admin*).

Main Menu

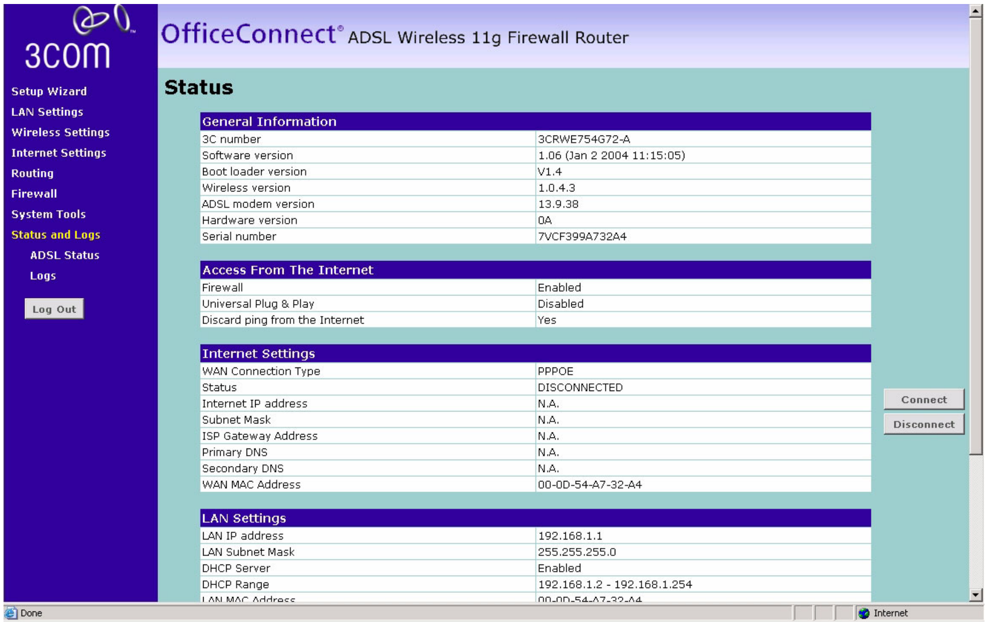
At the left side of all screens is a main menu, as shown in Figure 20 on page 36. When you click on a topic from the main menu, that page will appear in the main part of the screen.

Status Screen

The *Status* screen allows you to view a summary of the Router configuration, including the current Router status.

Status

Figure 20 Status Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
ADSL Status
Logs
Log Out
Status
Connect
Disconnect
Done
Internet

General Information	
3C number	3CRWE754G72-A
Software version	1.06 (Jan 2 2004 11:15:05)
Boot loader version	V1.4
Wireless version	1.0.4.3
ADSL modem version	13.9.38
Hardware version	0A
Serial number	7VCF399A732A4

Access From The Internet	
Firewall	Enabled
Universal Plug & Play	Disabled
Discard ping from the Internet	Yes

Internet Settings	
WAN Connection Type	PPPOE
Status	DISCONNECTED
Internet IP address	N.A.
Subnet Mask	N.A.
ISP Gateway Address	N.A.
Primary DNS	N.A.
Secondary DNS	N.A.
WAN MAC Address	00-0D-54-A7-32-A4

LAN Settings	
LAN IP address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP Server	Enabled
DHCP Range	192.168.1.2 - 192.168.1.254
LAN MAC Address	00-0D-54-A7-32-A4

There are two buttons on this screen - *Connect* and *Disconnect*. These buttons allow you to manually connect or disconnect your router from your ISP's service.

LAN Setup

Your Router is equipped with a DHCP server that will automatically assign IP addresses to each computer on your network. The factory default settings for the DHCP server will work in most any application. If you need to make changes to the settings, you can do so.

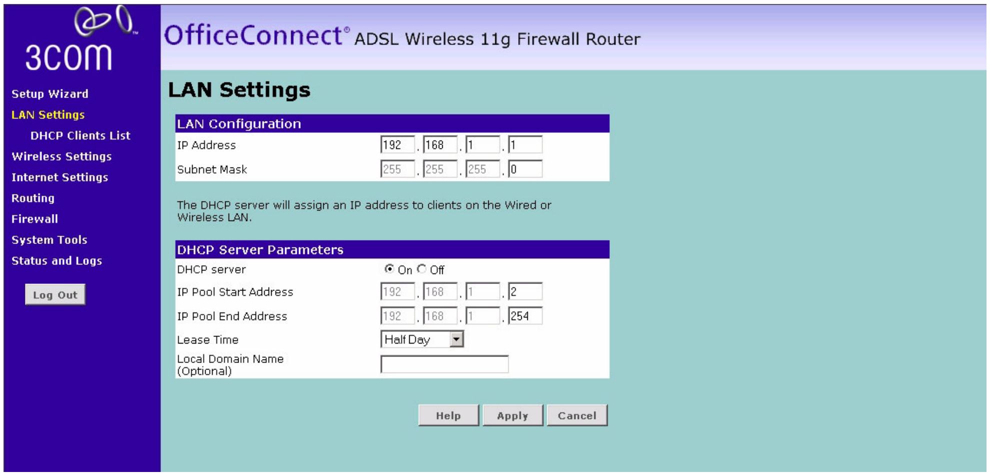
The changes that you can make are:

- Change the Internal IP address of the Router. The default = 192.168.1.1
- Change the Subnet Mask. The default = 255.255.255.0
- Enable/Disable the DHCP Server Function. Default = ON (Enabled)
- Specify the Starting and Ending IP Pool Address. Default = Starting: 2 / Ending: 254
- Specify the IP address Lease Time. Default = Half day
- Specify a local Domain Name. Default = NONE
- To make changes, click "LAN Settings" on the LAN tab to the left.

The Router will also provide you with a list of all client computers connected to the network. To view the list, click *DHCP clients list*.

LAN Settings

Figure 21 LAN Settings Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
DHCP Clients List
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

LAN Settings

LAN Configuration

IP Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

The DHCP server will assign an IP address to clients on the Wired or Wireless LAN.

DHCP Server Parameters

DHCP server ● On ○ Off

IP Pool Start Address 192 . 168 . 1 . 2

IP Pool End Address 192 . 168 . 1 . 254

Lease Time Half Day

Local Domain Name (Optional)

The LAN Settings screen is used to specify the LAN IP address of your Router, and to configure the DHCP server.

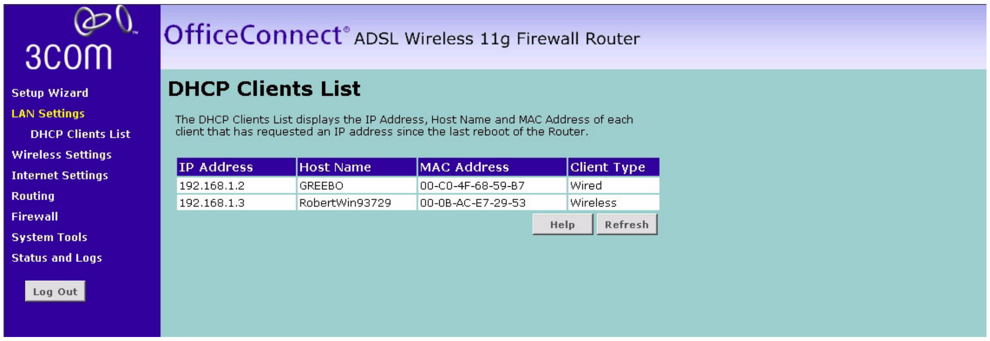
1. Select *LAN Settings* and then specify the Router *IP Address* and *Subnet Mask* in the appropriate fields. The default IP address of the Gateway is 192.168.1.1.
2. If you want to use the Gateway as a DHCP Server, click in the *On* check radio button.
3. If you need to, you can change the range of addresses given out by the Router by changing the *IP Pool Starting Address* and *IP Pool Ending Address* fields.
4. Specify the DHCP Lease time by selecting the required value from the *Lease Time* drop down list. The lease time is the length of time the DHCP server will reserve the IP address for each computer
5. Specify the Local Domain Name for your network.

   This step is optional.
6. Check all of your settings, and then click *Apply*.

The DHCP server will give out addresses to both wired and wireless clients.

DHCP Clients List

Figure 22 DHCP Clients List Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
DHCP Clients List
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Refresh

DHCP Clients List

The DHCP Clients List displays the IP Address, Host Name and MAC Address of each client that has requested an IP address since the last reboot of the Router.

IP Address	Host Name	MAC Address	Client Type
192.168.1.2	GREEBO	00-C0-4F-68-59-B7	Wired
192.168.1.3	RobertWin93729	00-0B-AC-E7-29-53	Wireless

The DHCP Clients List provides details on the devices that have received IP addresses from the Router. The list is only created when the Router is set up as a DHCP server. For each device that is connected to the LAN the following information is displayed:

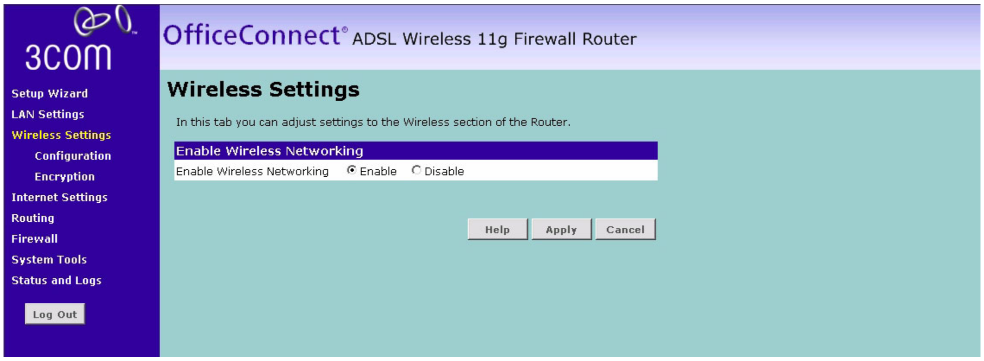
- IP address — The Internet Protocol (IP) address issued to the client machine.
- Host Name — The client machine's host name, if configured.
- MAC Address — The Media Access Control (MAC) address of the client's network card.

As you connect more devices, the client list will grow to a maximum number of 253 clients.

Wireless

From these pages you can configure the settings for wireless connections.

Figure 23 Wireless Settings Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Configuration
Encryption
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

Wireless Settings

In this tab you can adjust settings to the Wireless section of the Router.

Enable Wireless Networking

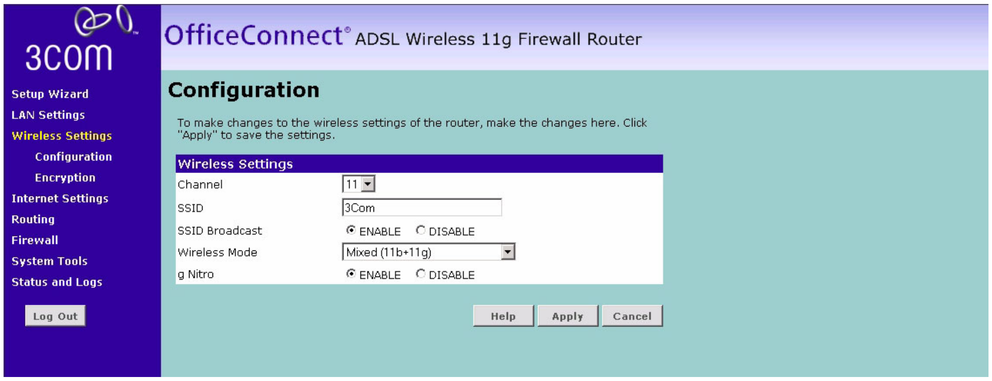
Enable Wireless Networking ● Enable ○ Disable

This screen allows you to enable or disable the wireless section of your LAN. When disabled, no wireless PCs can gain access to either the Internet or other PCs on your Wired or Wireless LAN through this Router.

Select the required setting, and press *Apply*.

Configuring Wireless

Figure 24 Wireless Configuration Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Configuration
Encryption
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

Configuration

To make changes to the wireless settings of the router, make the changes here. Click "Apply" to save the settings.

Wireless Settings	
Channel	11
SSID	3Com
SSID Broadcast	● ENABLE ○ DISABLE
Wireless Mode	Mixed (11b+11g)
g Nitro	● ENABLE ○ DISABLE

1 Set the Wireless Channel you want to use from the *Channel* drop-down list.

2 Specify the SSID to be used by your Wireless Network in the *SSID* field. If there are other wireless networks in your area, you should give your wireless network a unique name.

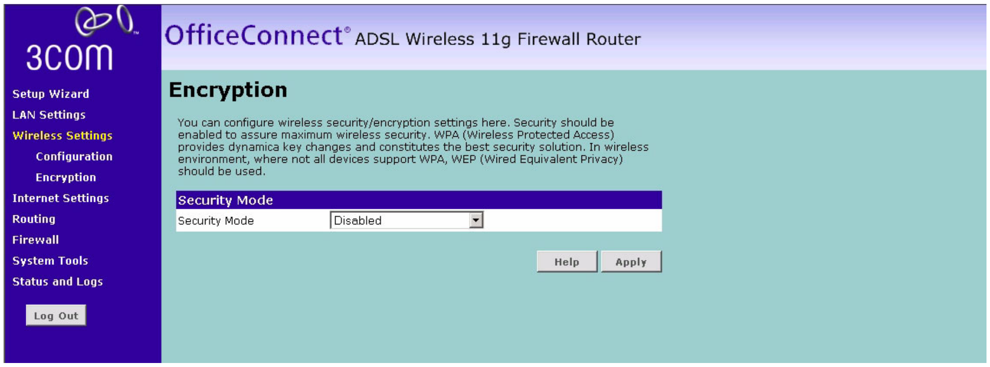
3 A feature of wireless networking is the ability for a wireless network adapter in a computer to look for an existing wireless network automatically. This is done by setting the card's SSID setting to "ANY".

Your Router is capable of blocking this "random" searching for a network. If you disable the "Broadcast SSID" feature, the only way a computer can join the network is by setting the computer's SSID to the specific name of the network (like WLAN). Be sure that you know your SSID (network name) before enabling this feature. It is possible to make your wireless network nearly invisible. By turning off the broadcast of the SSID, your network will not appear in a site survey. Site Survey is a feature of many wireless network adapters on the market today. It will scan the "air" for any available network and allow the computer to select the network from the site survey. Turning off the broadcast of the SSID will help increase security.

4. Select the Wireless Mode that you wish to use on your Router from the *Wireless Mode* drop down list. Unless you are having problems with your Wireless Network, it is recommended that you leave this setting on it's default value of *Mixed (11b+11g)*.
5. Select whether you wish to use g Nitro Mode on your Router by selecting the appropriate *g Nitro* radio button. Unless you are having problems with your Wireless Network, it is recommended that you leave this setting on it's default value of *Enable*.
6. Press *Apply*.

Encryption

Figure 25 Encryption Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Configuration
Encryption
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply

Encryption

You can configure wireless security/encryption settings here. Security should be enabled to assure maximum wireless security. WPA (Wireless Protected Access) provides dynamica key changes and constitutes the best security solution. In wireless environment, where not all devices support WPA, WEP (Wired Equivalent Privacy) should be used.

Security Mode

Security Mode: Disabled

From this screen, you can select the wireless security mode that you wish to use. There are five possible selections:

- Disabled (see page 41)
- WPA-PSK (no Server) (see page 41)
- 128-bit WEP (see page 42)

- 64-bit WEP (see page 42)
- WPA (with RADIUS Server) (see page 43)

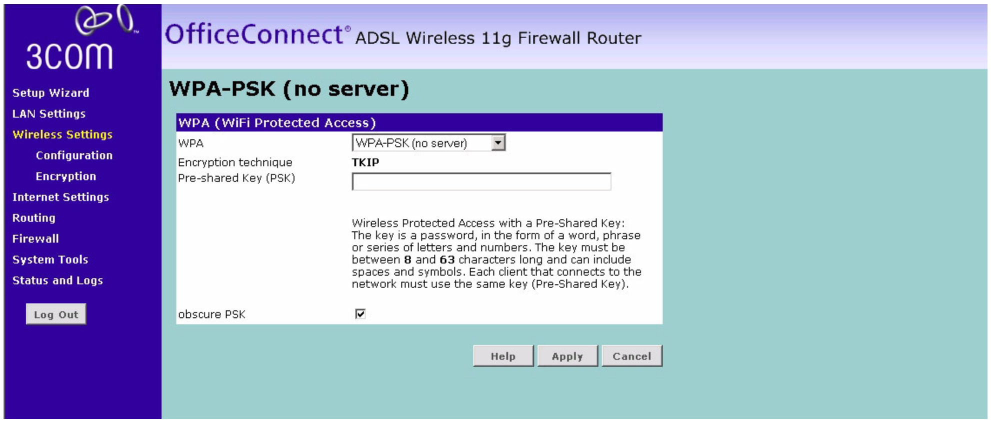
Select the required value from the drop down list, and press *Apply*.

Disabled

In this mode, wireless transmissions will not be encrypted, and will be visible to everyone. However, when setting up or debugging wireless networks it is often useful to use this security mode.

WPA-PSK (no server)

Figure 26 WPA-PSK (no server) Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Configuration
Encryption
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

WPA-PSK (no server)

WPA (WiFi Protected Access)

WPA: WPA-PSK (no server)
Encryption technique: **TKIP**
Pre-shared Key (PSK):

Wireless Protected Access with a Pre-Shared Key: The key is a password, in the form of a word, phrase or series of letters and numbers. The key must be between **8** and **63** characters long and can include spaces and symbols. Each client that connects to the network must use the same key (Pre-Shared Key).

obscure PSK ☑

WPA (Wireless Protected Access) provides dynamic key changes and constitutes the best security solution. In a wireless network where not all devices support WPA, WEP (Wired Equivalent Privacy) should be used.

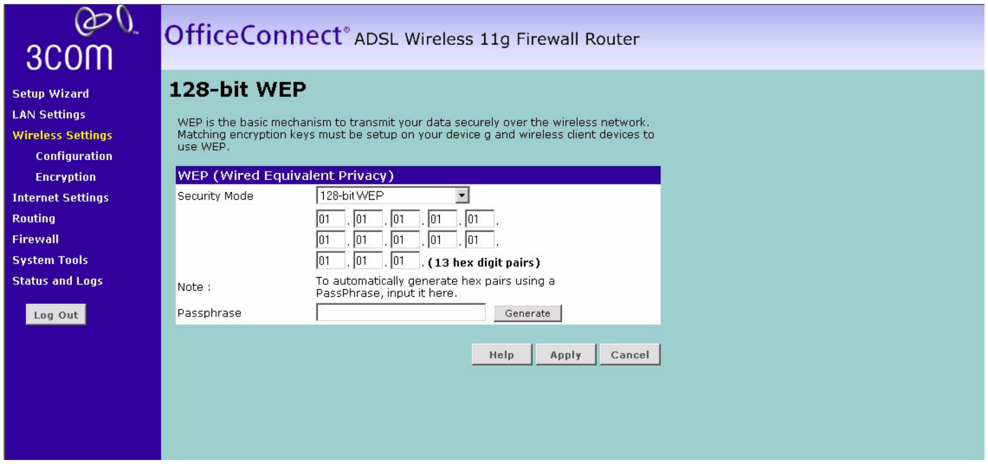
1. Enter the pre-shared key in the *Pre-shared Key (PSK)* field. The pre-shared key is a password, in the form of a word, phrase or series of letters and numbers. The key must be between 8 and 63 characters long and can include spaces and symbols.

   Note that each client that connects to the network must use the same key.

2. Click *Apply*.

128-bit WEP

Figure 27 128-bit WEP Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Configuration
Encryption
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Generate
Help
Apply
Cancel

128-bit WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your device g and wireless client devices to use WEP.

WEP (Wired Equivalent Privacy)

Security Mode: 128-bit WEP

01 . 01 . 01 . 01 . 01 .
01 . 01 . 01 . 01 . 01 .
01 . 01 . 01 . **(13 hex digit pairs)**

Note : To automatically generate hex pairs using a PassPhrase, input it here.

Passphrase

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your Router and wireless client devices to use WEP.

1 You can either enter your WEP key as 13 pairs of hex digits (0-9, A-F), or enter a memorable passphrase in the *Passphrase* box, and then click *Generate* to generate the hex keys from the passphrase.

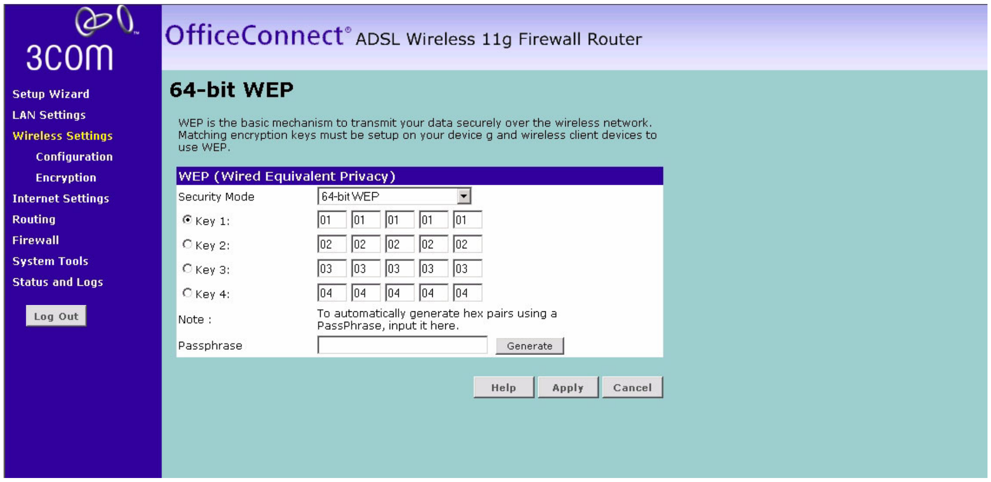
The WEP keys on each device in the wireless network must be identical.

In 128-bit WEP mode, only one WEP key (key 1) can be specified.

2 Click *Apply*.

64-bit WEP

Figure 28 64-bit WEP Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Configuration
Encryption
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Generate
Help
Apply
Cancel

64-bit WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your device g and wireless client devices to use WEP.

WEP (Wired Equivalent Privacy)

Security Mode: 64-bit WEP

● Key 1: 01 01 01 01 01
○ Key 2: 02 02 02 02 02
○ Key 3: 03 03 03 03 03
○ Key 4: 04 04 04 04 04

Note : To automatically generate hex pairs using a PassPhrase, input it here.

Passphrase

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your Router and wireless client devices to use WEP.

1 You can either enter your WEP key as 5 pairs of hex digits (0-9, A-F), or enter a memorable passphrase in the *Passphrase* box, and then click *Generate* to generate the hex keys from the passphrase.

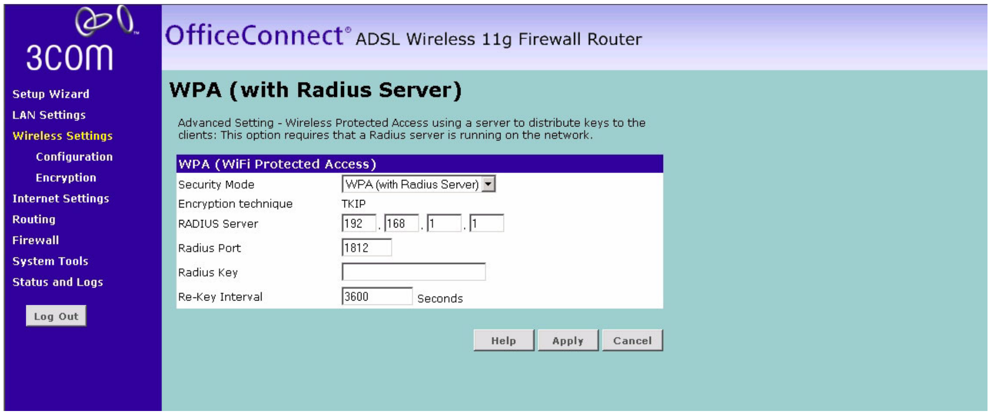
For 64-bit WEP, you can enter up to four keys, in the fields *Key 1* to *Key 4*. The radio button on the left hand side selects the key that is used in transmitting data.

Note that all four WEP keys on each device in the wireless network must be identical.

2 Click *Apply*.

WPA (with RADIUS Server)

Figure 29 WPA (with RADIUS Server) Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Configuration
Encryption
Internet Settings
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

WPA (with Radius Server)

Advanced Setting - Wireless Protected Access using a server to distribute keys to the clients: This option requires that a Radius server is running on the network.

WPA (WiFi Protected Access)

Security Mode: WPA (with Radius Server)
Encryption technique: TKIP
RADIUS Server: 192 . 168 . 1 . 1
Radius Port: 1812
Radius Key:
Re-Key Interval: 3600 Seconds

WPA (Wireless Protected Access) provides dynamic key changes and constitutes the best security solution. In a wireless network where not all devices support WPA, WEP (Wired Equivalent Privacy) should be used.

Wireless Protected Access using a server to distribute keys to the clients: This option requires that a Radius server is running on the network.

1 Enter the IP address of the RADIUS server on your network into the *RADIUS Server* field.

2 Enter the port that the RADIUS server is operating on in the *RADIUS Port* field.

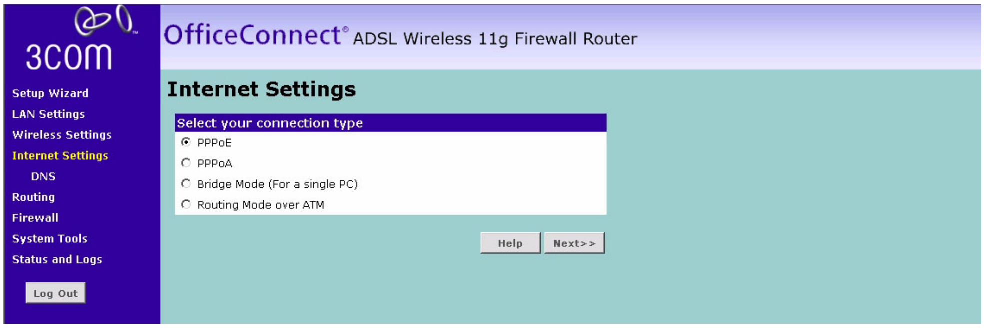
3. Enter the key for the RADIUS server in the *RADIUS Key* field.
4. By default, the WPA keys are changed every hour, but if you wish to change this you can do so by specifying the required time in the *Re-key Interval* field, in minutes
5. Click *Apply*.

Internet Settings

From these pages you can configure the settings for your DSL connection.

Connection Type

Figure 30 Connection Type Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
DNS
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Next>>

Internet Settings

Select your connection type

- ● PPPoE
- ○ PPPoA
- ○ Bridge Mode (For a single PC)
- ○ Routing Mode over ATM

The Connection Type screen is used to configured the parameters for your DSL connection. The information necessary to complete these screens should be obtained from your ISP.

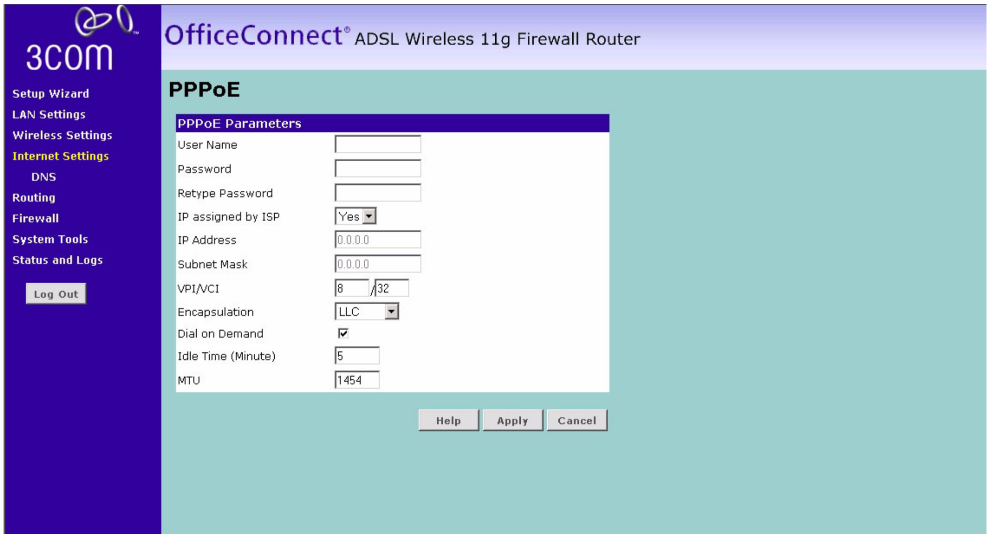
First, select the DSL connection mode from the four options available:

- PPPoE - PPP over Ethernet, providing routing for multiple PCs (see page 45)
- PPPoA - PPP over ATM, providing routing for multiple PCs (see page 46)
- Bridge Mode (for a single PC) - RFC1483 Bridged Mode, for single PCs only (see page 47)
- Routing Mode over ATM - RFC1483 Routed Mode, for multiple PCs (see page 47)

Click *Next*.

PPPoE

Figure 31 PPPoE Settings Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
DNS
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

PPPoE

PPPoE Parameters

User Name
Password
Retype Password
IP assigned by ISP: Yes
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
VPI/VCI: 8 / 32
Encapsulation: LLC
Dial on Demand: ☑
Idle Time (Minute): 5
MTU: 1454

1. Enter the User Name assigned to you by your ISP in the *User Name* field.
2. Enter the Password assigned to you by your ISP in the *Password* field. Re-enter your password in the *Retype Password* field.
3. If your ISP assigns your IP address dynamically, then select *Yes* in the *IP assigned by ISP* field and proceed to step 4. If your ISP has assigned you a fixed or static IP address, select *No* in the *IP assigned by ISP* field.

   Then enter the IP address and Subnet Mask information provided by your ISP into the *IP address* and *Subnet Mask* fields.

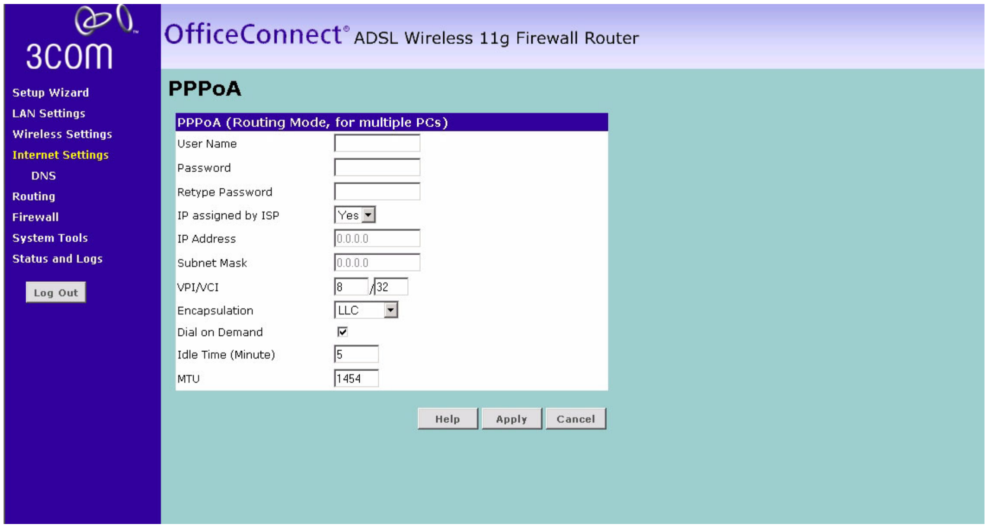
4. Enter the VPI and VCI parameters provided to you by your ISP in the *VPI* and *VCI* fields.
5. Select the encapsulation type (LLC or VC MUX) in the *Encapsulation Type* field. This information will have been provided to you by your ISP.
6. If you want your Router to connect to the Internet every time a PC needs to access it, check the *Dial on Demand* checkbox. If this box is not checked, then you will have to manually connect and disconnect using the buttons on the Status Screen (see page 35).
7. If you want your Router to automatically disconnect from the Internet automatically after a period of inactivity, specify a time in the *Idle Time (Minutes)* field.

   Enter a value of 0 to disable this timeout.

8 Click *Apply*.

PPPoA

Figure 32 PPPoA Settings Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
DNS
Routing
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

PPPoA

PPPoA (Routing Mode, for multiple PCs)

User Name	
Password	
Retype Password	
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
VPI/VCI	8 / 32
Encapsulation	LLC
Dial on Demand	☑
Idle Time (Minute)	5
MTU	1454

1 Enter the User Name assigned to you by your ISP in the *User Name* field.

2 Enter the Password assigned to you by your ISP in the *Password* field. Re-enter your password in the *Retype Password* field.

3 If your ISP assigns your IP address dynamically then select *Yes* in the *IP assigned by ISP* field and proceed to step 4. If your ISP has assigned you a fixed or static IP address, select *No* in the *IP assigned by ISP* field.

Then enter the IP address and Subnet Mask information provided by your ISP into the *IP address* and *Subnet Mask* fields.

4 Enter the VPI and VCI parameters provided to you by your ISP in the *VPI* and *VCI* fields.

5 Select the encapsulation type (LLC or VC MUX) in the *Encapsulation Type* field. This information will have been provided to you by your ISP.

6 If you want your Router to connect to the Internet every time a PC needs to access it, check the *Dial on Demand* checkbox. If this box is not checked, then you will have to manually connect and disconnect using the buttons on the Home Screen (see page 35).

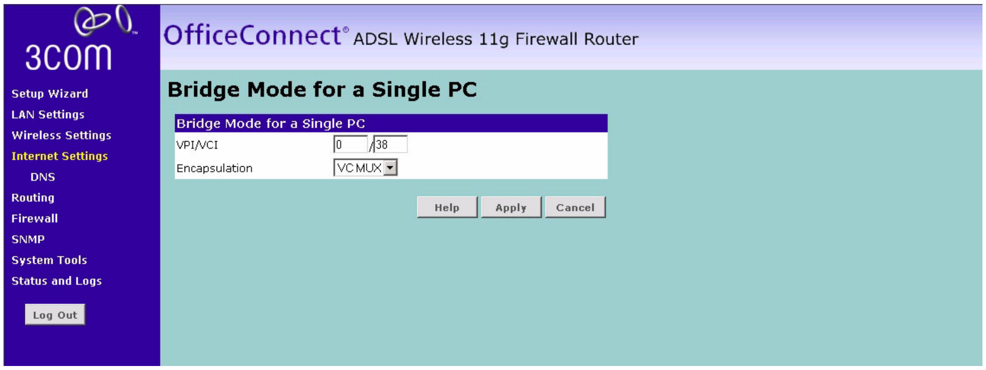
7 If you want your Router to automatically disconnect from the Internet automatically after a period of inactivity, specify a time in the *Idle Time (Minutes)* field.

Enter a value of 0 to disable this timeout.

8 Click *Apply*.

Bridged Mode for Single PC

Figure 33 Bridge Mode for Single PC Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
DNS
Routing
Firewall
SNMP
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

Bridge Mode for a Single PC

Bridge Mode for a Single PC

VPI/VCI	0 / 38
Encapsulation	VC MUX

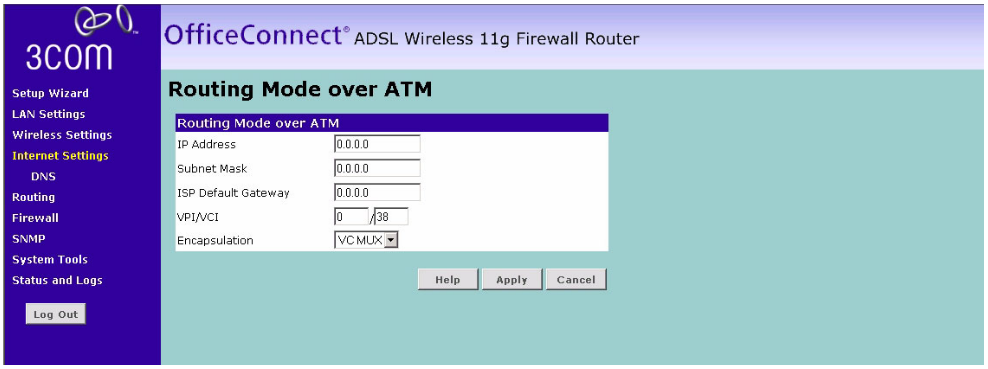
1 Enter the VPI and VCI parameters provided to you by your ISP in the *VPI* and *VCI* fields.

2 Select the encapsulation type (LLC or VC MUX) in the *Encapsulation Type* field. This information will have been provided to you by your ISP.

3 Click *Apply*.

Routing Mode over ATM

Figure 34 Routing Mode over ATM Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
DNS
Routing
Firewall
SNMP
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

Routing Mode over ATM

Routing Mode over ATM

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
ISP Default Gateway	0.0.0.0
VPI/VCI	0 / 38
Encapsulation	VC MUX

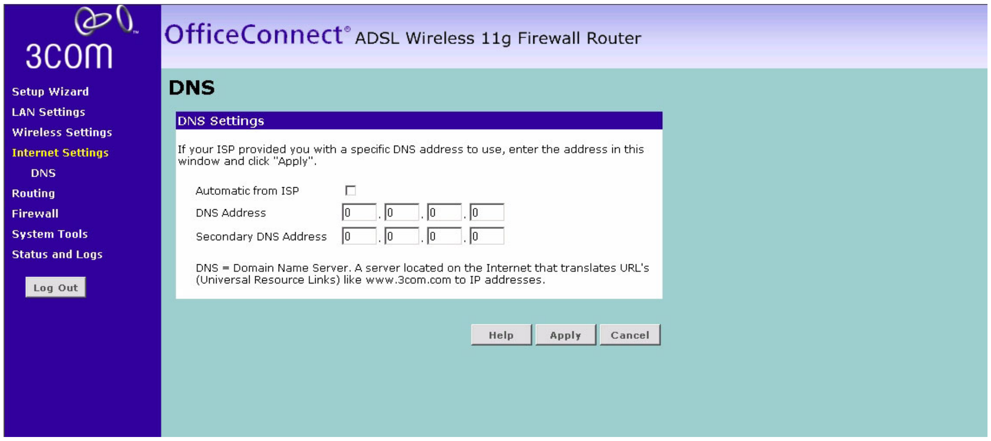
1 Enter the IP address, Subnet Mask and Default Gateway information provided by your ISP into the *IP address*, *Subnet Mask* and *Default Route* fields.

2 Enter the VPI and VCI parameters provided to you by your ISP in the *VPI* and *VCI* fields.

3. Select the encapsulation type (LLC or VC MUX) in the *Encapsulation* field. This information will have been provided to you by your ISP.
4. Click *Apply*.

DNS

Figure 35 DNS Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
DNS
Routing
Firewall
System Tools
Status and Logs
Log Out
DNS
DNS Settings
Help
Apply
Cancel

If your ISP provided you with a specific DNS address to use, enter the address in this window and click "Apply".

Automatic from ISP ☐
DNS Address 0 . 0 . 0 . 0
Secondary DNS Address 0 . 0 . 0 . 0

DNS = Domain Name Server. A server located on the Internet that translates URL's (Universal Resource Links) like www.3com.com to IP addresses.

If your ISP provided you with specific DNS addresses to us, enter them into the appropriate fields on this screen and click *Apply*.

Many ISP's do not require you to enter this information into the Router. If you are using a Static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is Dynamic, PPPoA or PPPoE, it is likely that you do not have to enter a DNS address.

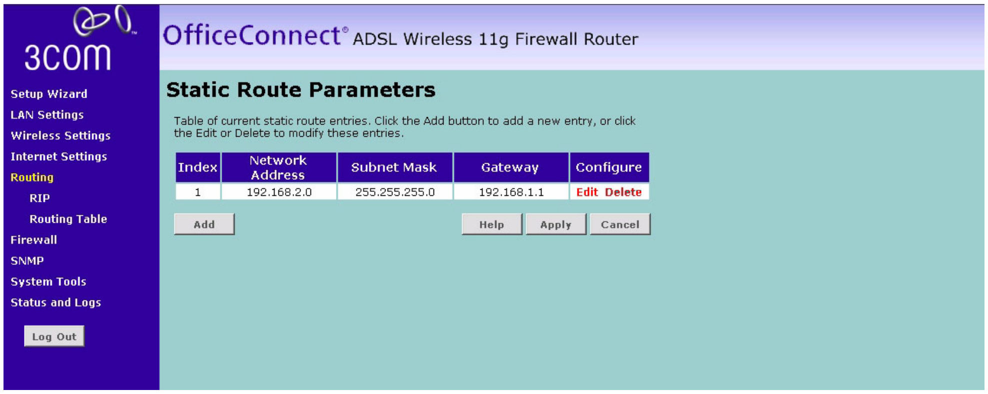
Routing

From these pages you can configure routing parameters. Your Router supports the following routing functionality:

- Static Routing
- RIP (Routing Information Protocol) — RIP allows the network administrator to set up routing information on one RIP-enabled device and send that information to all RIP-enabled devices on the network.
- Routing table display.

Static Routes

Figure 36 Static Route Parameters Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
RIP
Routing Table
Firewall
SNMP
System Tools
Status and Logs
Log Out
Add
Help
Apply
Cancel

Static Route Parameters

Table of current static route entries. Click the Add button to add a new entry, or click the Edit or Delete to modify these entries.

Index	Network Address	Subnet Mask	Gateway	Configure
1	192.168.2.0	255.255.255.0	192.168.1.1	Edit Delete

The Static Route Parameter screen shows a list of current static route entries. For each entry, the following information is displayed:

- *Index* — the index of the entry
- *Network Address* — the network address of the route.
- *Subnet Mask* — the subnet mask of the route.

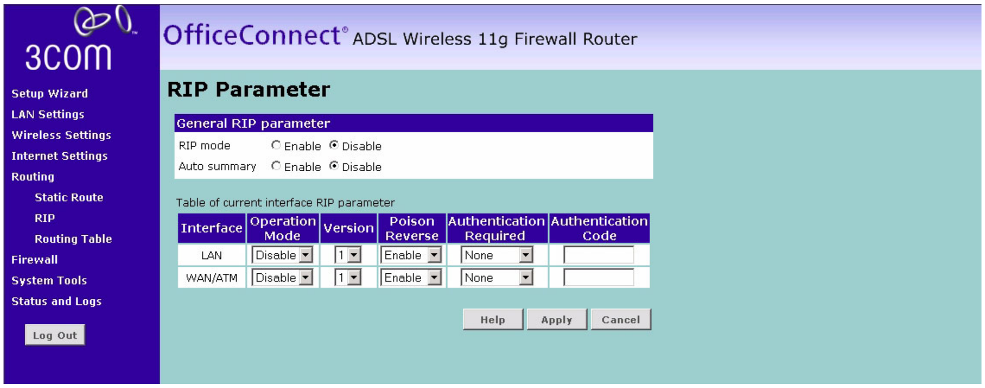
A network address of 0.0.0.0 and a subnet mask of 0.0.0.0 indicates the default route.

- *Gateway* — the gateway used to route data to the network specified by the network address.

To add a static route entry to the table, type in the network address, subnet mask and gateway, and click *Add.* To change an entry, click *Edit* and to delete an entry, click *Delete*. After you have finished making changes to the table, click *Apply*.

RIP Parameters

Figure 37 RIP Parameter Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Static Route
RIP
Routing Table
Firewall
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

RIP Parameter

General RIP parameter

RIP mode ○ Enable ● Disable

Auto summary ○ Enable ● Disable

Table of current interface RIP parameter

Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Authentication Code
LAN	Disable	1	Enable	None	
WAN/ATM	Disable	1	Enable	None	

You can set up RIP independently on both LAN and WAN interfaces.

1. Select the RIP Mode *Enable* radio button.
2. Select the appropriate radio button to enable or disable *Auto Summary*. Auto Summarization sends simplified routing data to other RIP-enabled devices rather than full routing data.
3. Select the *Operation Mode*:
   - Disabled — RIP is not enabled for the WAN or LAN interface.
   - Enabled — RIP is enabled for the WAN or LAN interface. The router will transmit RIP update information to other RIP-enabled devices.
   - Silent — RIP is enabled, however the router only receives RIP update messages, it will not transmit any messages itself.
4. In the Version field, select *RIPv1* or *RIPv2*.

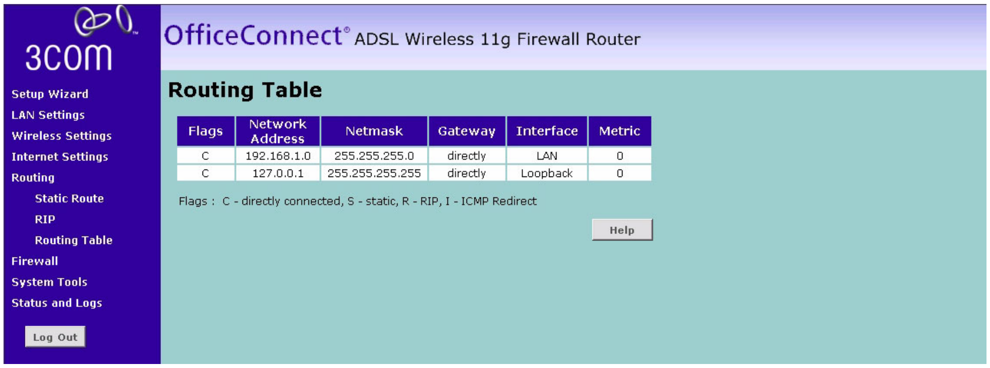
We recommend that you only use RIPv1 if there is an existing RIP-enabled device on your network that does not support RIPv2. In all other cases, you should use RIPv2.

5. Use the *Poison Reverse* radio button to enable or disable Poison reverse on the router. Enabling Poison Reverse on your Router allows it to indicate to other RIP-enabled devices that they have both routes that point to each other, preventing data loops.
6. Use the *Authentication Required* field to choose one of three modes of authentication:
   - None — Switches off authentication on the specified interface.
   - Password — An unencrypted text password that needs to be set on all RIP-enabled devices connected to this router. RIP information is not shared between devices whose passwords do not match.
   - MD5 — A password that has been encrypted using the MD5 encryption algorithm that needs to be set on all RIP-enabled devices connected to this router. RIP information is not shared between devices whose passwords do not match.
7. In the *Authentication Code* field, enter the password that is required if either the *Password* or *MD5* option has been selected.
8. Click *Apply*.

Routing Table

The Routing Table screen displays details for the default routing used by your Router and any routing created using Static Routing or RIP.

Figure 38 Routing Table Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Static Route
RIP
Routing Table
Firewall
System Tools
Status and Logs
Log Out
Help

Routing Table

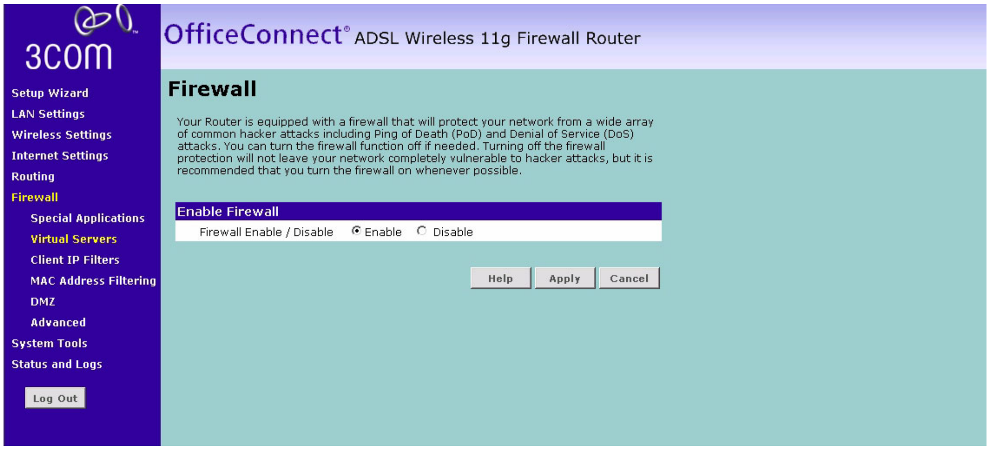
Flags	Network Address	Netmask	Gateway	Interface	Metric
C	192.168.1.0	255.255.255.0	directly	LAN	0
C	127.0.0.1	255.255.255.255	directly	Loopback	0

Flags : C - directly connected, S - static, R - RIP, I - ICMP Redirect

Firewall

From these pages you can configure settings for the firewall.

Figure 39 Firewall Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

Firewall

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

Enable Firewall

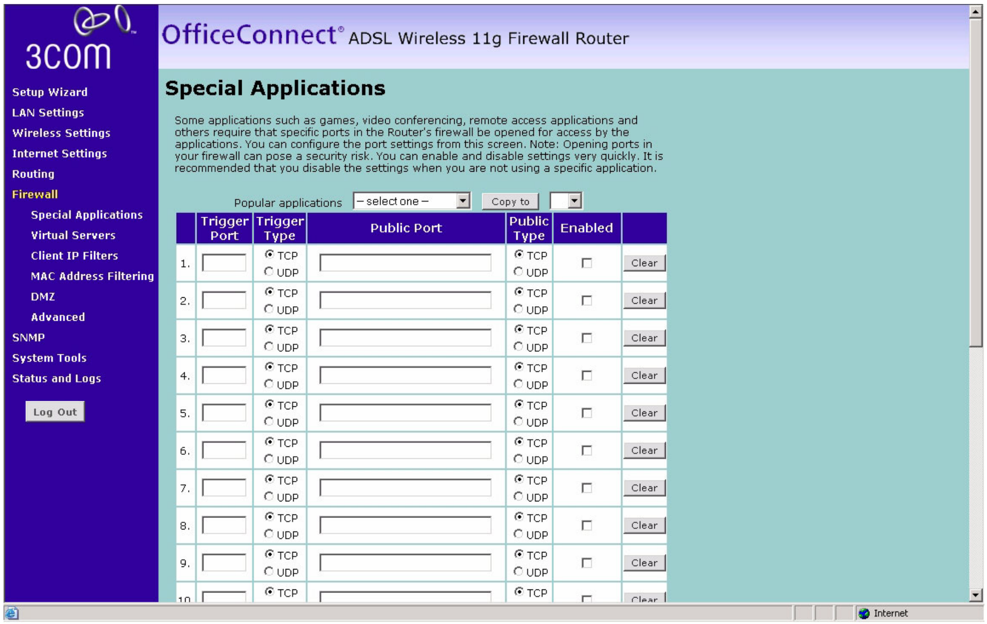
Firewall Enable / Disable ● Enable ○ Disable

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.

1. Enable or Disable the Firewall as required by selecting the appropriate radio button.
2. Press *Apply*.

Special Applications

Figure 40 Special Applications Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
SNMP
System Tools
Status and Logs
Log Out
Internet

Special Applications

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen. Note: Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application.

Popular applications – select one – Copy to

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled	
1.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
2.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
3.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
4.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
5.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
6.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
7.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
8.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
9.		● TCP ○ UDP		● TCP ○ UDP	☐	Clear
10		● TCP		● TCP	☐	Clear

Special Applications let you specify specific ports to be open for specific applications to work properly with the Network Address Translation (NAT) feature of the Router.

A list of popular applications has been included to choose from. Select your application from the drop-down list at the top of the screen. Select the row that you want to copy the settings to from the drop-down list, select the row you want to copy to, and then click *Copy To*. The settings will be transferred to the row you specified. Click *Apply* to save the setting for that application.

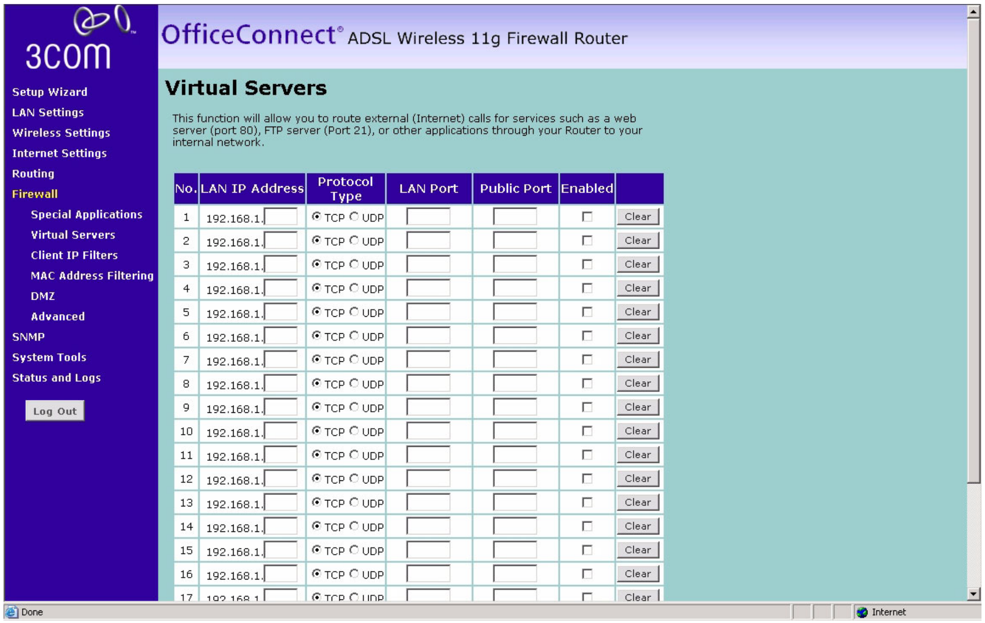
If your application is not here, you will need to check with the application vendor to determine which ports need to be configured. You can manually input this port information into the Router. To do this:

1. Specify the trigger port (the one used by the application when it is initialized) in the *Trigger Port* column, and specify whether the trigger is TCP or UDP.
2. Specify the Public Ports used by the application, that will need to be opened up in the firewall for the application to work properly. Also specify whether these ports are TCP or UDP.
3. You can temporarily enable or disable each entry in the table by checking or unchecking the *Enabled* checkbox.

4 Click *Apply.*

Virtual Servers

Figure 41 Virtual Servers Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
SNMP
System Tools
Status and Logs
Log Out
Done
Internet

Virtual Servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network.

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enabled	
1	192.168.1.	● TCP ○ UDP			☐	Clear
2	192.168.1.	● TCP ○ UDP			☐	Clear
3	192.168.1.	● TCP ○ UDP			☐	Clear
4	192.168.1.	● TCP ○ UDP			☐	Clear
5	192.168.1.	● TCP ○ UDP			☐	Clear
6	192.168.1.	● TCP ○ UDP			☐	Clear
7	192.168.1.	● TCP ○ UDP			☐	Clear
8	192.168.1.	● TCP ○ UDP			☐	Clear
9	192.168.1.	● TCP ○ UDP			☐	Clear
10	192.168.1.	● TCP ○ UDP			☐	Clear
11	192.168.1.	● TCP ○ UDP			☐	Clear
12	192.168.1.	● TCP ○ UDP			☐	Clear
13	192.168.1.	● TCP ○ UDP			☐	Clear
14	192.168.1.	● TCP ○ UDP			☐	Clear
15	192.168.1.	● TCP ○ UDP			☐	Clear
16	192.168.1.	● TCP ○ UDP			☐	Clear
17	192.168.1.	● TCP ○ UDP			☐	Clear

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be 'seen'.

If you need to configure the Virtual Server function for a specific application, you will need to contact the application vendor to find out which port settings you need.

To manually enter settings:

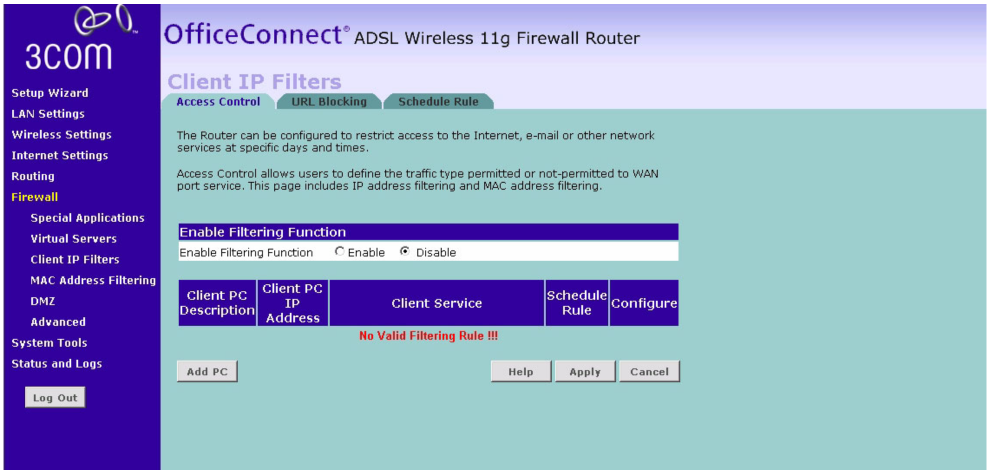
1. Enter the IP address in the space provided for the internal machine.
2. Enter the port type (TCP, UDP, or both TCP and UDP).
3. Specify the Public port that will be seen by clients on the Internet, and the LAN port which the traffic will be routed to.
4. You can enable or disable each Virtual Server entry by checking or unchecking the appropriate *Enable* checkbox.
5. Click *Apply* to save the changes for each Virtual Server entry.

Client IP Filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

Access Control

Figure 42 Access Control Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
Client IP Filters
Access Control
URL Blocking
Schedule Rule
Add PC
Help
Apply
Cancel

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times.

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function

Enable Filtering Function ○ Enable ● Disable

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure

No Valid Filtering Rule !!!

Access Control allows users to define the traffic type permitted or not-permitted to the Internet.

This screen allows you to enable or disable all Access Control rules. Select the appropriate *Enable Filtering Function* radio button, and click *Apply* to save the settings.

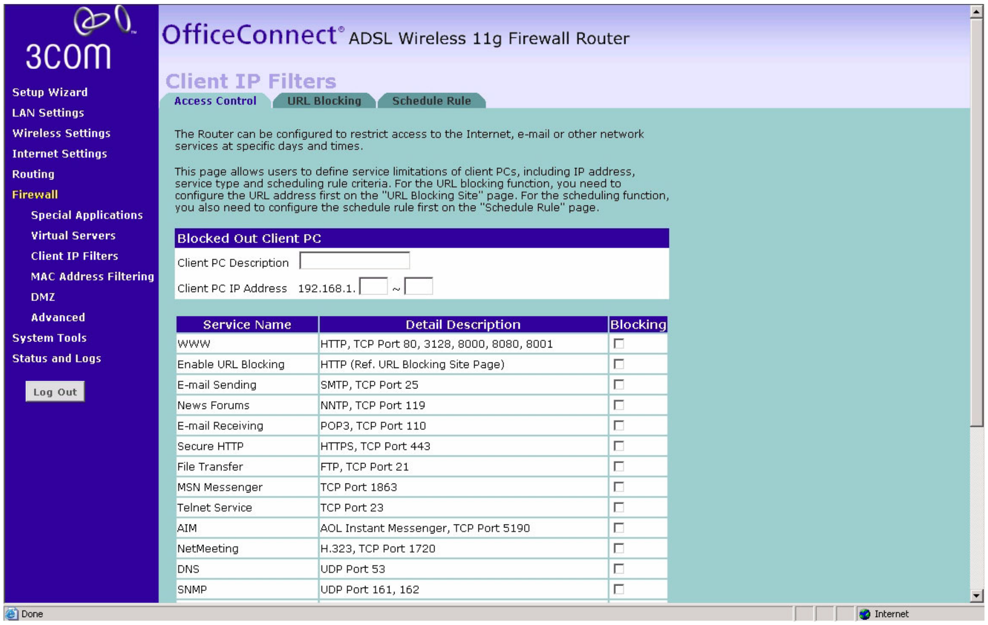
To edit or delete specific Access Control rules, click on *Edit* or *Delete* for the appropriate access control rule.

To control access to specific Internet services:

1 Click on *Add PC.*

A screen similar to that shown below will appear

Figure 43 Add PC Screen


3com
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
OfficeConnect® ADSL Wireless 11g Firewall Router
Client IP Filters
Access Control
URL Blocking
Schedule Rule
Done
Internet

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times.

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Blocked Out Client PC

Client PC Description

Client PC IP Address 192.168.1. ~

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	☐
Enable URL Blocking	HTTP (Ref. URL Blocking Site Page)	☐
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☐
MSN Messenger	TCP Port 1863	☐
Telnet Service	TCP Port 23	☐
AIM	AOL Instant Messenger, TCP Port 5190	☐
NetMeeting	H.323, TCP Port 1720	☐
DNS	UDP Port 53	☐
SNMP	UDP Port 161, 162	☐

2 Enter a description for the filter you are defining in the *Client PC Description* field.

3 Enter the IP address or IP address range into the *Client IP Address* fields.

4 Select the services to be blocked. A list of popular services is given on this screen, to block a particular service place a check in the appropriate *Blocking* checkbox.

If the service to be restricted is not listed on the screen, you can enter a custom range of ports at the bottom of the page, under *User Defined Service*.

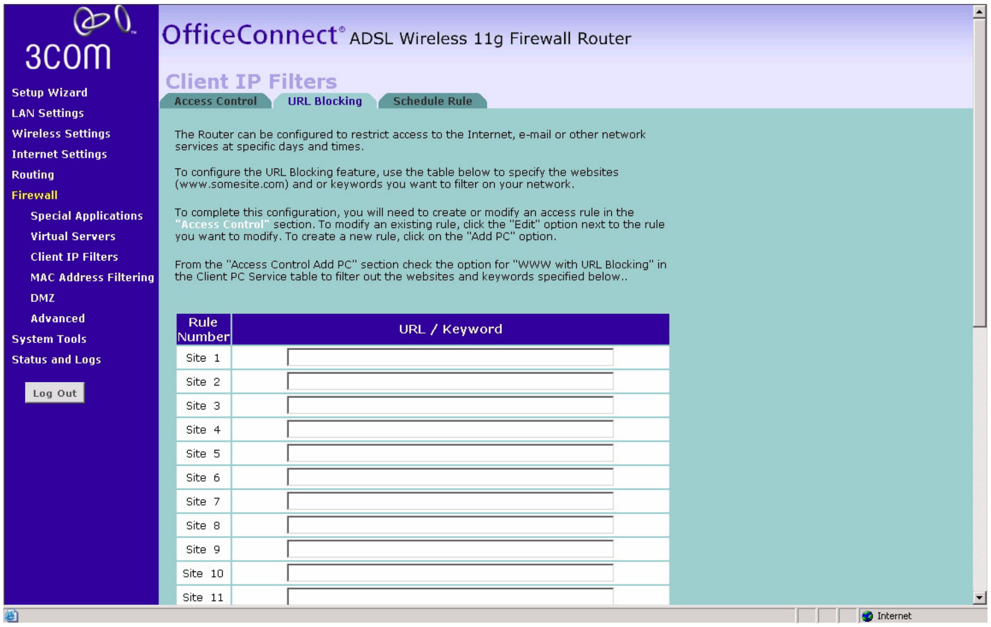
5 If you want the restriction to only apply at certain times, select the schedule rule to apply from the *Schedule Rule* drop down list.

Note that Schedule Rules are defined on the Schedule Rule page (see page 57).

6 Click *OK* to add the settings.

URL Blocking

Figure 44 URL Blocking Screen


3com
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
OfficeConnect® ADSL Wireless 11g Firewall Router
Client IP Filters
Access Control
URL Blocking
Schedule Rule
Internet

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times.

To configure the URL Blocking feature, use the table below to specify the websites (www.somesite.com) and or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section. To modify an existing rule, click the "Edit" option next to the rule you want to modify. To create a new rule, click on the "Add PC" option.

From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below..

Rule Number	URL / Keyword
Site 1	
Site 2	
Site 3	
Site 4	
Site 5	
Site 6	
Site 7	
Site 8	
Site 9	
Site 10	
Site 11	

To configure the URL Blocking feature, use the table on the URL Blocking page to specify the websites (www.somesite.com) and/or keywords you want to filter on your network.

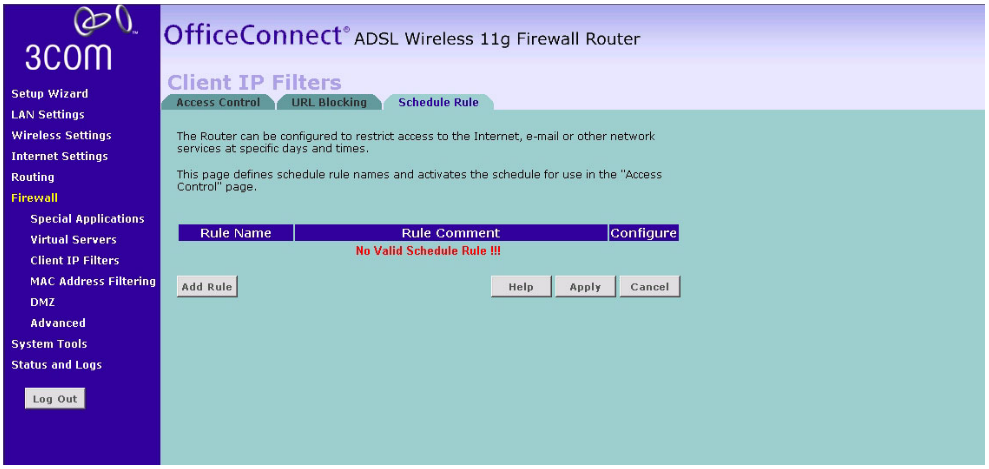
For example, entering a keyword of “xxx” would block access to any URL that contains the string “xxx”.

To complete this configuration, you will need to create or modify an access rule in the "Access Control" section (see “Access Control” on page 54).

From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified in the table.

Schedule Rule

Figure 45 Schedule Rule Screen


3com
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
OfficeConnect® ADSL Wireless 11g Firewall Router
Client IP Filters
Access Control
URL Blocking
Schedule Rule
Add Rule
Help
Apply
Cancel

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times.

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Rule Name	Rule Comment	Configure
	No Valid Schedule Rule !!!	

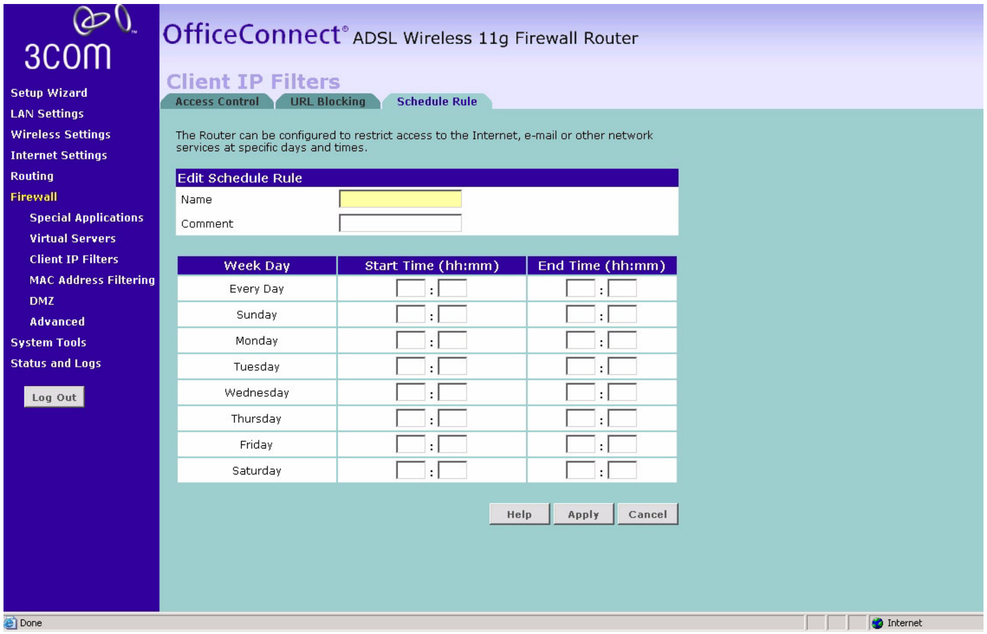
The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. These schedule rules are used by the rules defined on the Access Control page (see "Access Control" on page 54).

To add a schedule rule:

1 Click *Add Rule*

A screen similar to that shown below will appear.

Figure 46 Add Schedule Rule Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Client IP Filters
Access Control
URL Blocking
Schedule Rule
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
Help
Apply
Cancel
Done
Internet

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times.

Edit Schedule Rule

Name	
Comment	

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	:	:
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:

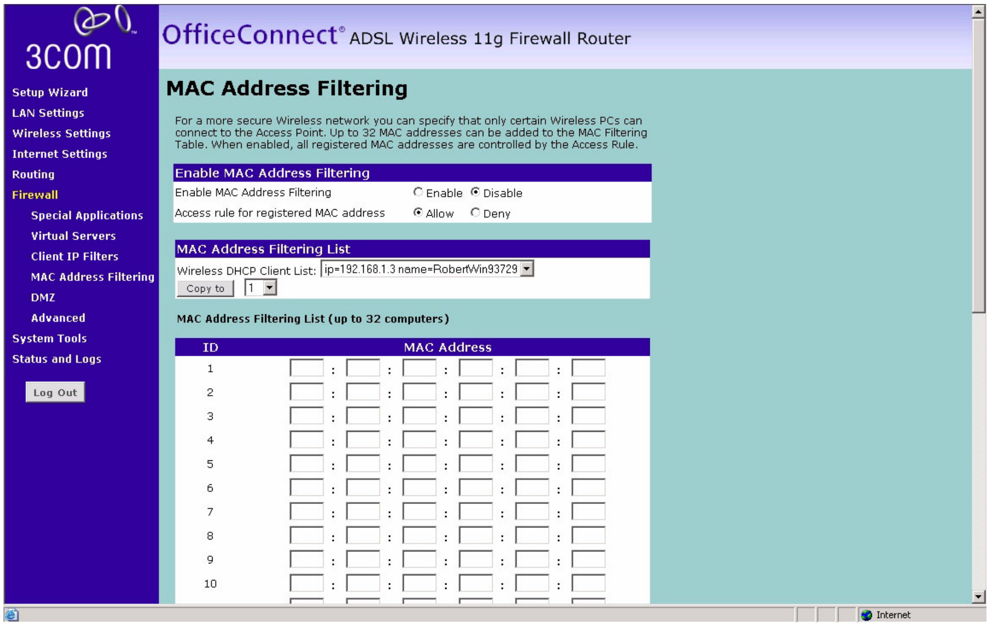
2 Enter a name and comment for the schedule rule in the *Name* and *Comment* fields.

3 Specify the schedule rules for the required days and times - note that all times should be in 24 hour format.

4 Click *Apply*.

MAC Address Filtering

Figure 47 MAC Address Filtering Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
Copy to
Internet

MAC Address Filtering

For a more secure Wireless network you can specify that only certain Wireless PCs can connect to the Access Point. Up to 32 MAC addresses can be added to the MAC Filtering Table. When enabled, all registered MAC addresses are controlled by the Access Rule.

Enable MAC Address Filtering

Enable MAC Address Filtering ○ Enable ● Disable

Access rule for registered MAC address ● Allow ○ Deny

MAC Address Filtering List

Wireless DHCP Client List: ip=192.168.1.3 name=RobertWin93729

Copy to 1

MAC Address Filtering List (up to 32 computers)

ID	MAC Address
1	: : : : :
2	: : : : :
3	: : : : :
4	: : : : :
5	: : : : :
6	: : : : :
7	: : : : :
8	: : : : :
9	: : : : :
10	: : : : :

The MAC Address Filter is a powerful security feature that allows you to specify which computers are allowed on the Wireless network. Any wireless computers attempting to access the network that are not specified in the filter list will be denied access.

To Enable or Disable this feature, select the appropriate *Enable MAC Address Filtering* radio button, and click *Apply*.

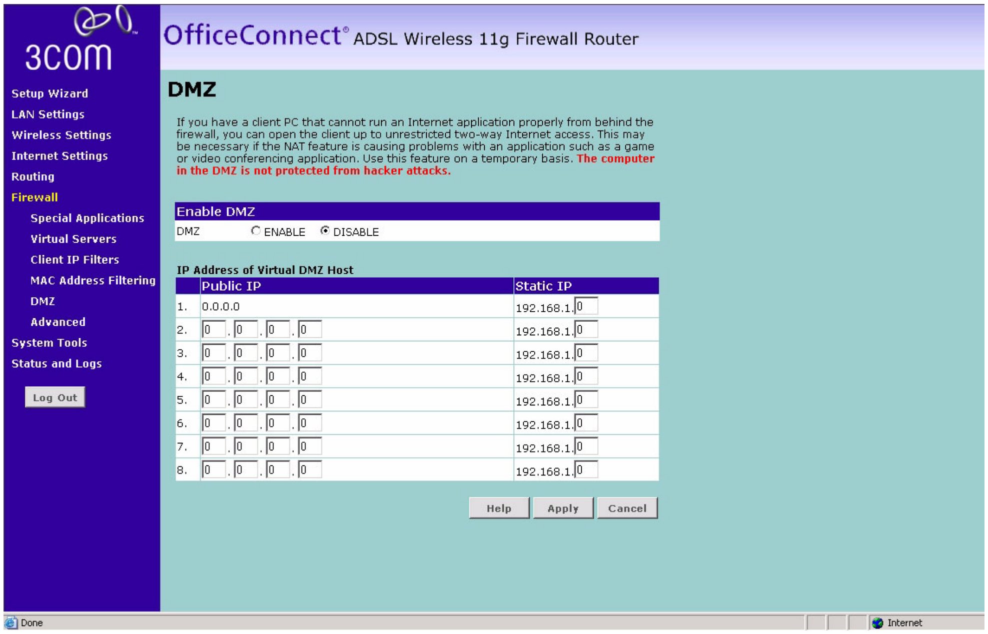
When you enable this feature, you must enter the MAC address of each client on your network to allow network access.

Alternatively, you can copy the MAC address by selecting the name of the computer from the *DHCP Clients List*, and then location in the MAC Address Filter table, and then click *Copy To*.

Click *Apply* to save the settings.

DMZ

Figure 48 DMZ Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
Help
Apply
Cancel
Done
Internet

DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. **The computer in the DMZ is not protected from hacker attacks.**

Enable DMZ

DMZ ○ ENABLE ● DISABLE

IP Address of Virtual DMZ Host

	Public IP	Static IP
1.	0.0.0.0	192.168.1.0
2.	0 . 0 . 0 . 0	192.168.1.0
3.	0 . 0 . 0 . 0	192.168.1.0
4.	0 . 0 . 0 . 0	192.168.1.0
5.	0 . 0 . 0 . 0	192.168.1.0
6.	0 . 0 . 0 . 0	192.168.1.0
7.	0 . 0 . 0 . 0	192.168.1.0
8.	0 . 0 . 0 . 0	192.168.1.0

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application.

Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

To put a computer in the DMZ, enter the last digits of its LAN IP address in the *Static IP* field. Put the IP address (if known) that will be accessing the DMZ PC into the *Public IP* field, so that only the computer on the Internet at this address can access this PC without firewall protection. If the IP address is not known, or if more than one PC on the Internet will need to access this PC, then set the *Public IP* to *0.0.0.0*.

Click *Apply*.

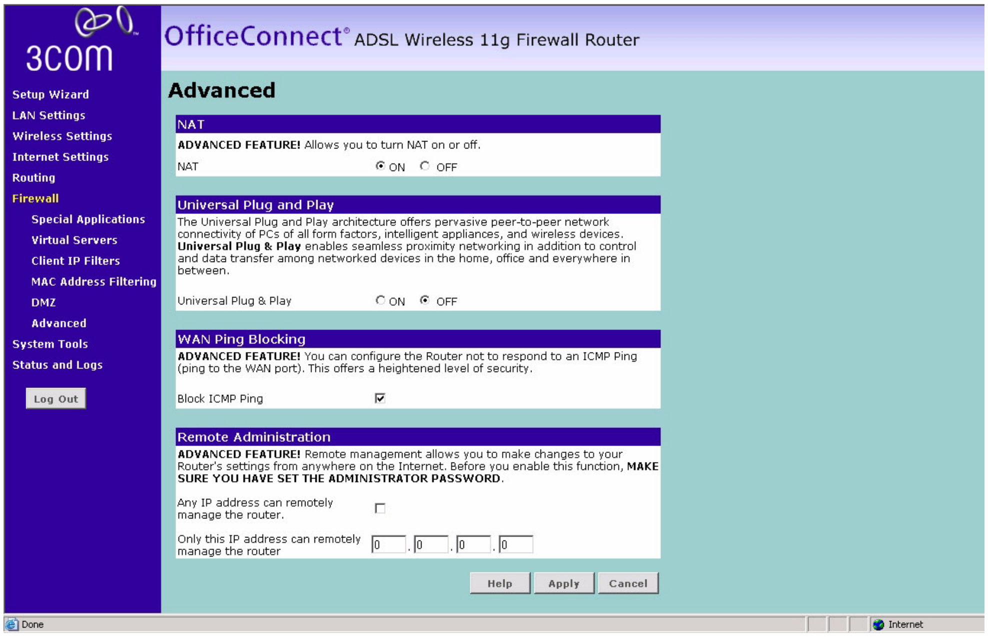
Advanced

From the Advanced screen, you can configure:

- NAT (Network Address Translation)
- Universal Plug and Play
- WAN Ping Blocking

- Remote Admin

Figure 49 Advanced Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
Special Applications
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
Advanced
System Tools
Status and Logs
Log Out
Help
Apply
Cancel
Done
Internet

Advanced

NAT

ADVANCED FEATURE! Allows you to turn NAT on or off.

NAT ● ON ○ OFF

Universal Plug and Play

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. **Universal Plug & Play** enables seamless proximity networking in addition to control and data transfer among networked devices in the home, office and everywhere in between.

Universal Plug & Play ○ ON ● OFF

WAN Ping Blocking

ADVANCED FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to the WAN port). This offers a heightened level of security.

Block ICMP Ping ☑

Remote Administration

ADVANCED FEATURE! Remote management allows you to make changes to your Router's settings from anywhere on the Internet. Before you enable this function, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD**.

Any IP address can remotely manage the router. ☐

Only this IP address can remotely manage the router 0 . 0 . 0 . 0

NAT Enable

Before you enable this function, make sure you have changed the administrator password. Network Address Translation (NAT) is the method by which the router shares the single IP address assigned by your ISP with the computers on your network. This function should only be used by advanced users, and if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur.

Universal Plug and Play

Universal Plug and Play is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are Universal Plug and Play compliant. Some applications require the Router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports and in some instances setting trigger ports. An application that is Universal Plug and Play compliant has the ability to communicate with the Router, basically "telling" the Router which way it needs the firewall configured. The

Router ships with the Universal Plug and Play feature disabled. If you are using any applications that are Universal Plug and Play compliant, and wish to take advantage of the Universal Plug and Play features, you can enable this feature. Simply select *Enable* in the *UPnP Enabling* section of the Utilities page. Click *Apply* to save the change.

WAN Ping Blocking

Computer hackers use what is known as "Pinging" to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there.

The Router can be set up so it will not respond to an ICMP Ping from the outside. This heightens the level of security of your Router.

To turn off the ping response, select *Block ICMP Ping* and click *Apply;* the router will not respond to an ICMP ping from the Internet.

Remote Administration

Before you enable this function, ensure that you have set the Administration Password.

Remote Administration allows you to make changes to your Router’s settings from anywhere on the Internet. You can choose to either:

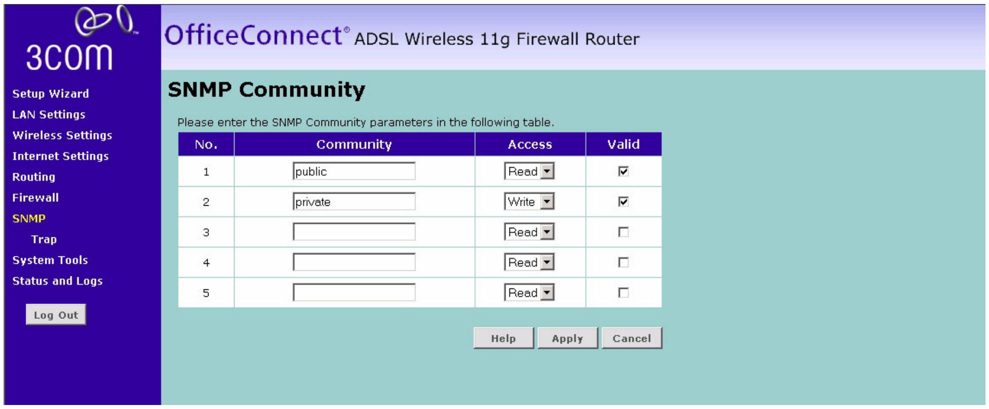
- Click the check box to enable any PC on the network to remotely manage your Router
- Enter one specific IP address that can remotely manage your router. This is more secure, as only the specified IP address will be able to manage the Router

SNMP

SNMP (Simple Network Management Protocol) allows remote management of your router by a PC that has an SNMP management agent installed.

SNMP Community

Figure 50 SNMP Community Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
SNMP
Trap
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

SNMP Community

Please enter the SNMP Community parameters in the following table.

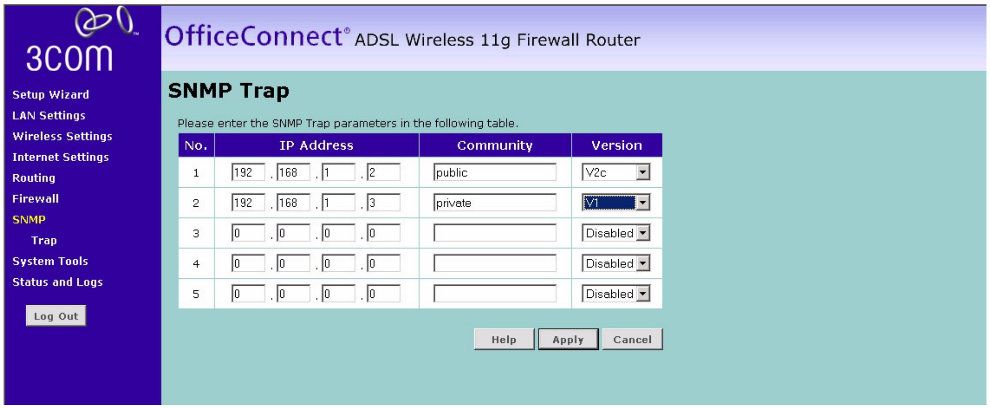
No.	Community	Access	Valid
1	public	Read	☑
2	private	Write	☑
3		Read	☐
4		Read	☐
5		Read	☐

To Configure SNMP:

1. In the *Community* column, enter the name of the SNMP communication channel. Your SNMP management agent needs to be configured with this name so that it can communicate with your router.
2. In the *Access* column, select *Read* to allow the management agent to collect data (for example, bandwidth usage) from your router. Select *Write* to allow the management agent to change the configuration of your router.
3. Check the appropriate *Valid* checkbox to enable the communication channel.

SNMP Trap

Figure 51 SNMP Trap Screen


3com
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
SNMP
Trap
System Tools
Status and Logs
Log Out
Help
Apply
Cancel

OfficeConnect® ADSL Wireless 11g Firewall Router

SNMP Trap

Please enter the SNMP Trap parameters in the following table.

No.	IP Address	Community	Version
1	192 . 168 . 1 . 2	public	V2c
2	192 . 168 . 1 . 3	private	V1
3	0 . 0 . 0 . 0		Disabled
4	0 . 0 . 0 . 0		Disabled
5	0 . 0 . 0 . 0		Disabled

You can configure your router to send status messages to the SNMP management agent if a problem occurs on the network. To configure traps:

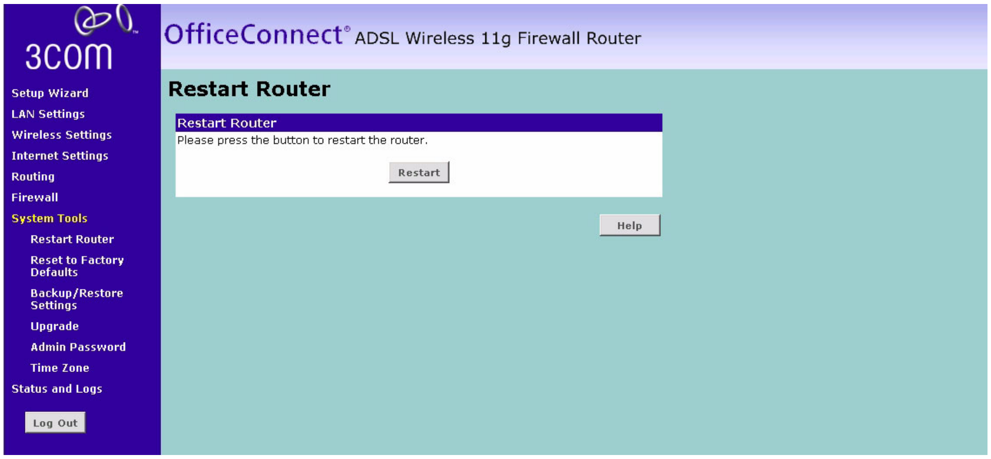
1. In the *IP Address* field, enter the IP address of the PC to which you want your router to send status messages.
2. In the *Community* field, enter the name of the SNMP communication channel to which you want your router to send status messages.
3. Set the Version field to match the version of trap messaging that your SNMP management agent supports. The router supports V1 and V2c trap messaging.

System Tools

These pages lets you manage different parameters of the router and perform certain administrative functions.

Restart Router

Figure 52 Restart Router Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Restart Router
Reset to Factory Defaults
Backup/Restore Settings
Upgrade
Admin Password
Time Zone
Status and Logs
Log Out
Restart Router
Restart Router
Restart
Help

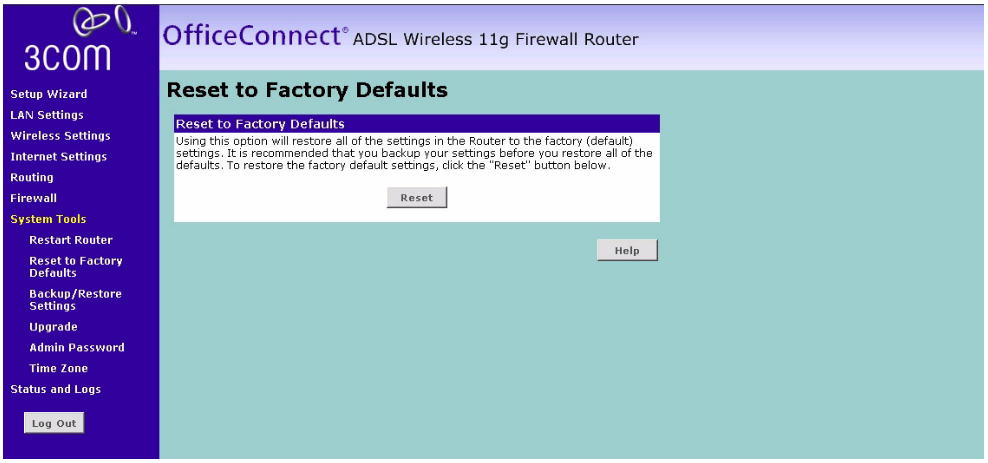
Please press the button to restart the router.

Sometimes it may be necessary to Restart or Reboot the Router. Restarting or Rebooting the Router will not delete any of your configuration settings.

Click *Restart* to Restart or Reboot the Router.

Reset to Factory Default

Figure 53 Reset to Factory Default Screen

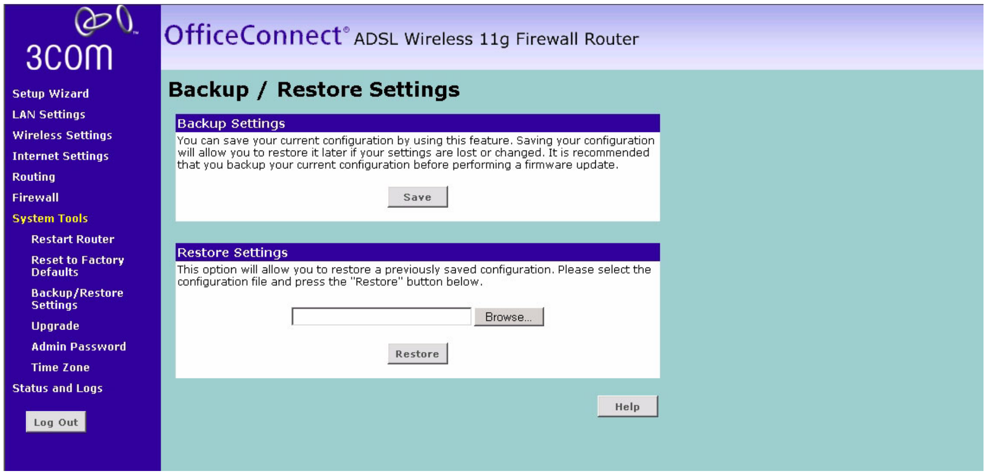

3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Restart Router
Reset to Factory Defaults
Backup/Restore Settings
Upgrade
Admin Password
Time Zone
Status and Logs
Log Out
Reset to Factory Defaults
Reset to Factory Defaults
Reset
Help

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click the "Reset" button below.

Using this option will reset all of the settings in the Router to the factory (default) settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click *Reset*.

Backup/Restore Settings

Figure 54 Backup/Restore Settings Screen


3com
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Restart Router
Reset to Factory Defaults
Backup/Restore Settings
Upgrade
Admin Password
Time Zone
Status and Logs
Log Out
Save
Browse...
Restore
Help

OfficeConnect® ADSL Wireless 11g Firewall Router

Backup / Restore Settings

Backup Settings

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

Restore Settings

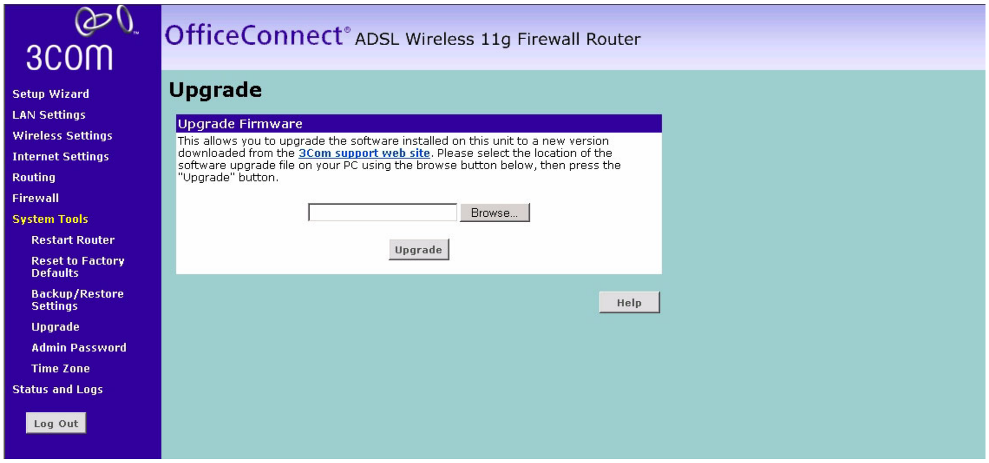
This option will allow you to restore a previously saved configuration. Please select the configuration file and press the "Restore" button below.

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

This option will allow you to restore a previously saved configuration. Please select the configuration file and click *Restore*.

Upgrade

Figure 55 Upgrade Screen


3com
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Restart Router
Reset to Factory Defaults
Backup/Restore Settings
Upgrade
Admin Password
Time Zone
Status and Logs
Log Out
Browse...
Upgrade
Help

OfficeConnect® ADSL Wireless 11g Firewall Router

Upgrade

Upgrade Firmware

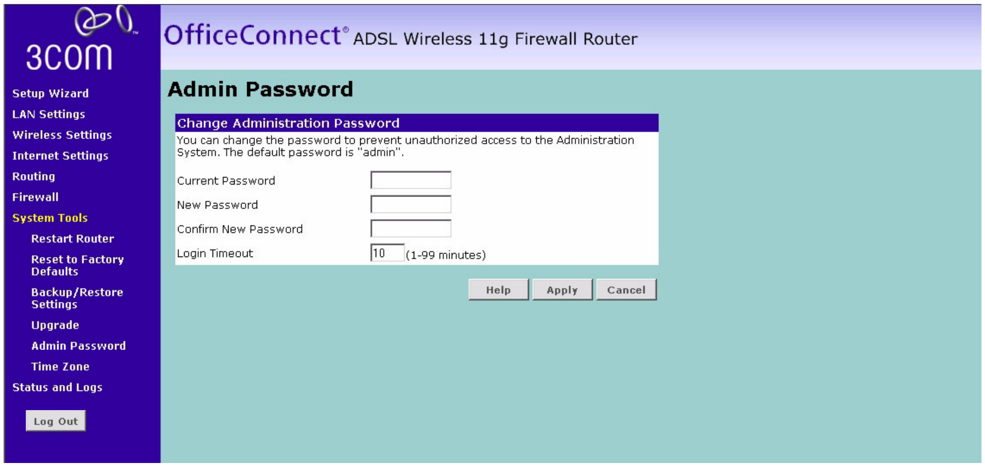
This allows you to upgrade the software installed on this unit to a new version downloaded from the 3Com support web site. Please select the location of the software upgrade file on your PC using the browse button below, then press the "Upgrade" button.

From time to time 3Com may release new versions of the Routers firmware. Firmware updates contain improvements and fixes to problems that may have existed.

Please download the firmware file to your PC first, and then click *Browse* and select the firmware file. Click *Upgrade* to upload the firmware to the Router.

Admin Password

Figure 56 Admin Password Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Restart Router
Reset to Factory Defaults
Backup/Restore Settings
Upgrade
Admin Password
Time Zone
Status and Logs
Log Out
Help
Apply
Cancel

Admin Password

Change Administration Password

You can change the password to prevent unauthorized access to the Administration System. The default password is "admin".

Current Password
New Password
Confirm New Password
Login Timeout 10 (1-99 minutes)

The Router ships with a default password of *admin*. 3Com recommends that you change the password for added security. Keep your password in a safe place as you will need this password to log into the router in the future. It is also recommended that you set a password if you plan to use the Remote management feature of this Router.

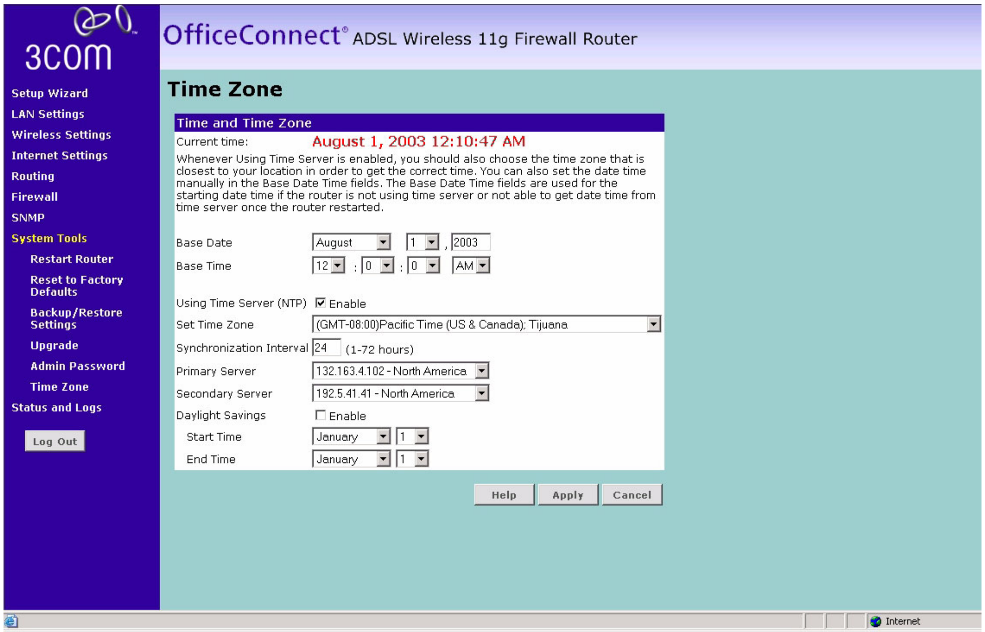
To change the password:

1. Enter the current password into the *Type in current password* field.
2. Enter the new password into the *Type in new Password* and *Confirm new Password* fields.
3. Click *Apply*.

The login timeout option allows you to set the period of time that you can be logged into the Router's setup interface. The timer starts when there is no activity. For example, you have made some changes in the setup interface, then left your computer alone without clicking "Logout". Assuming the timeout is set to 5 minutes, then 5 minutes after you leave, the login session will expire. You will have to login to the router again to make any more changes. The login timeout option is for security purposes and the default is set to 5 minutes. As a note, only one computer can be logged into the Router's web management interface at one time.

Time and Time Zone

Figure 57 Time and Time Zone screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
SNMP
System Tools
Restart Router
Reset to Factory Defaults
Backup/Restore Settings
Upgrade
Admin Password
Time Zone
Status and Logs
Log Out
Help
Apply
Cancel
Internet

Time Zone

Time and Time Zone

Current time: August 1, 2003 12:10:47 AM

Whenever Using Time Server is enabled, you should also choose the time zone that is closest to your location in order to get the correct time. You can also set the date time manually in the Base Date Time fields. The Base Date Time fields are used for the starting date time if the router is not using time server or not able to get date time from time server once the router restarted.

Base Date: August 1, 2003
Base Time: 12 : 0 : 0 AM
Using Time Server (NTP): ☑ Enable
Set Time Zone: (GMT-08:00)Pacific Time (US & Canada); Tijuana
Synchronization Interval: 24 (1-72 hours)
Primary Server: 132.163.4.102 - North America
Secondary Server: 192.5.41.41 - North America
Daylight Savings: ☐ Enable
Start Time: January 1
End Time: January 1

The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in. If you reside in an area that observes Daylight Saving, then place a checkmark in the box next to "Enable Daylight Saving". The system clock may not update immediately. Allow at least 15 minutes for the router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

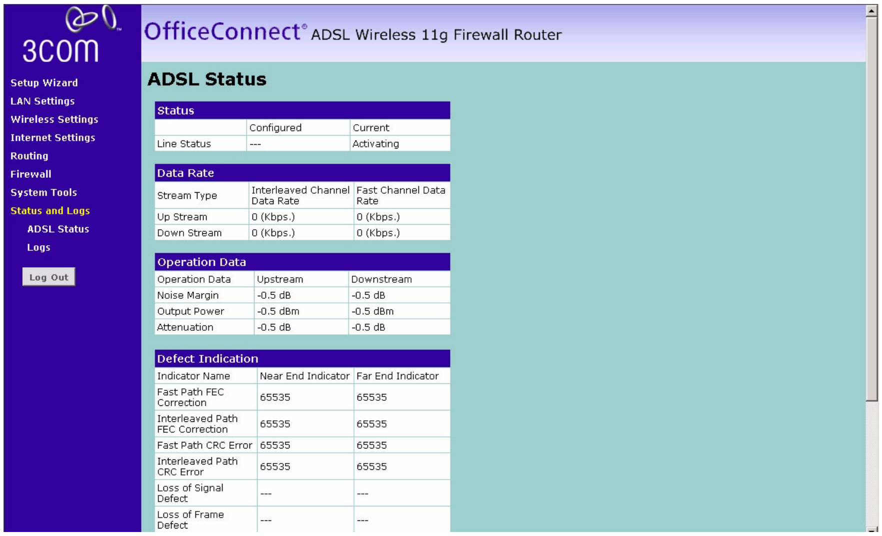
You can specify which SNTP servers the Router will use to update it's system clock, although doing this should only be necessary if you are experiencing difficulty.

Status and Logs

You can use the Status pages to view version numbers for your router’s software and hardware and check the status of connections to WAN, LAN and WLAN interfaces.

ADSL Status

Figure 58 ADSL Status Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
ADSL Status
Logs
Log Out

ADSL Status

Status		
	Configured	Current
Line Status	---	Activating

Data Rate		
Stream Type	Interleaved Channel Data Rate	Fast Channel Data Rate
Up Stream	0 (Kbps.)	0 (Kbps.)
Down Stream	0 (Kbps.)	0 (Kbps.)

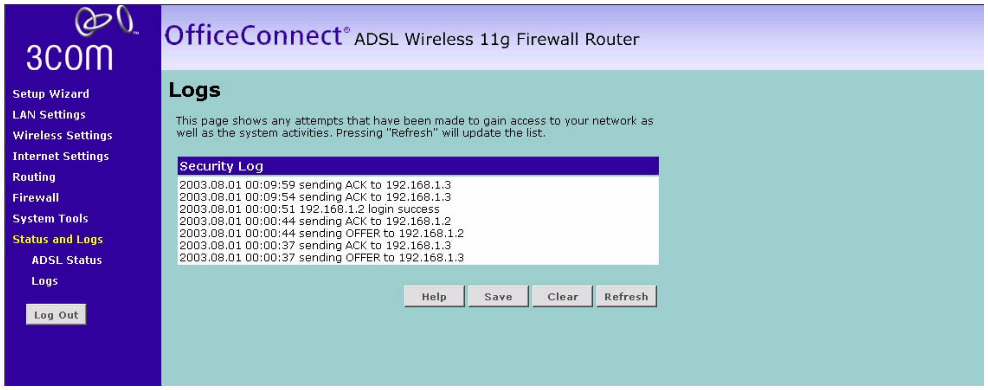
Operation Data		
Operation Data	Upstream	Downstream
Noise Margin	-0.5 dB	-0.5 dB
Output Power	-0.5 dBm	-0.5 dBm
Attenuation	-0.5 dB	-0.5 dB

Defect Indication		
Indicator Name	Near End Indicator	Far End Indicator
Fast Path FEC Correction	65535	65535
Interleaved Path FEC Correction	65535	65535
Fast Path CRC Error	65535	65535
Interleaved Path CRC Error	65535	65535
Loss of Signal Defect	---	---
Loss of Frame Defect	---	---

This screen shows modem status and statistics

Logs

Figure 59 Logs Screen


3com
OfficeConnect® ADSL Wireless 11g Firewall Router
Setup Wizard
LAN Settings
Wireless Settings
Internet Settings
Routing
Firewall
System Tools
Status and Logs
ADSL Status
Logs
Log Out
Help
Save
Clear
Refresh

Logs

This page shows any attempts that have been made to gain access to your network as well as the system activities. Pressing "Refresh" will update the list.

Security Log

```
2003.08.01 00:09:59 sending ACK to 192.168.1.3
2003.08.01 00:09:54 sending ACK to 192.168.1.3
2003.08.01 00:00:51 192.168.1.2 login success
2003.08.01 00:00:44 sending ACK to 192.168.1.2
2003.08.01 00:00:44 sending OFFER to 192.168.1.2
2003.08.01 00:00:37 sending ACK to 192.168.1.3
2003.08.01 00:00:37 sending OFFER to 192.168.1.3
```

This screen shows any attempts that have been made to gain access to your network as well as the system activities.

Click *Refresh* to update the display.

Click *Clear* to clear the log (note that all current entries will be erased).

Click *Save* to save the log to disk in a text file. When prompted for a location to save the file to, specify a filename and location, and then click *OK*.

6 TROUBLESHOOTING

Basic Connection Checks

- Check that the Router is connected to your computers and to the telephone line, and that all the equipment is powered on. Check that the LAN Status and DSL LEDs on the Router are illuminated, and that any corresponding LEDs on the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

Browsing to the Router Configuration Screens

If you have connected your Router and computers together but cannot browse to the Router configuration screens, check the following:

- Confirm that the physical connection between your computer and the Router is OK, and that the LAN Status LEDs on the Gateway and NIC are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.
- Ensure that you have configured your computer as described in Chapter 3, *Setting Up Your Computers*. Restart your computer while it is connected to the Router to ensure that your computer receives an IP address.
- When entering the address of the Router into your web browser, ensure that you use the full URL including the http:// prefix (e.g. **`http://192.168.1.1`**).
- Ensure that you do not have a Web proxy enabled on your computer. Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click on the *LAN Settings* button at the bottom. Make sure that the *Proxy Server* option is unchecked.

- If you cannot browse to the Router, use the *winipcfg* utility in Windows 95/98/ME to verify that your computer has received the correct address information from the Router. From the *Start* menu, choose *Run* and then enter **`winipcfg`**. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Router is 192.168.1.1 (the address of the Gateway). If these are not correct, use the *Release* and *Renew* functions to obtain a new IP address from the Router. Under Windows 2000 and Windows XP, use the *ipconfig* command-line utility to perform the same functions.

Connecting to the Internet

If you can browse to the Router configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Router and the telephone line is OK, and that the DSL LED on the Router is illuminated.
- Ensure that you have entered the correct information into the Router configuration screens as required by your Internet Service Provider. Use the “Internet Settings” screen to verify this.
- Check that the PPPoE or PPPoA user name and password are correct.
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under *Control Panel* > *Internet Options* > *Connections*.

Forgotten Password and Reset to Factory Defaults

If you can browse to the Router configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Router to it’s factory default configuration.

***CAUTION:** All your configuration changes will be lost, and you will need to run the configuration wizard again before you can re-establish your Router connection to the Internet. Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.*

1. Remove power from the Router.
2. Disconnect all your computers and the telephone line from the Router.
3. Re-apply power to the Router, and wait for it to finish booting up.

4. Press and hold the *Reset* button on the rear panel (see “Rear Panel” on page 15) for 5 seconds.
5. The Router will restart, and when the start-up sequence has completed, browse to:

   `http://192.168.1.1`

   and run the configuration wizard. You may need to restart your computer before you attempt this.
6. When the configuration wizard has completed, you may reconnect your network as it was before.

Wireless Networking

- Ensure that you have an 802.11b or 802.11g wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each Wireless computer has either Windows 95 or higher or MAC OS 8.5 or higher.
- Verify that your wireless computers are configured to work in Infrastructure mode and not Ad Hoc mode. The Router contains an Access Point that is designed to operate in Infrastructure mode. Ad Hoc mode is not supported by the Router.
- If you have a wired and a wireless NIC in the same computer, ensure that the wired NIC is disabled.
- Check the status of the Router Wireless LED, it should be lit if wireless is enabled and will flash when there is wireless activity. If not lit go to “Wireless” on page 39 and enable wireless networking.
- Ensure that the TCP/IP settings for all devices are correct.
- Ensure that the Wireless Clients are using the same SSID or Service Area Name as the Router. The SSID is case-sensitive
- Ensure that the encryption method and level that you use on your clients are the same as those configured on the Router. The Router cannot simultaneously support WPA and WEP encryption.
- Ensure that you have the Wireless computer enabled in the list of allowed MAC addresses if you are using MAC Address Filtering on the Router.
- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Router. For more effective coverage you can try reorientating your antennae. Place one antenna vertically and one horizontally to improve coverage.

Additionally consider moving the wireless computer closer to the Router to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the Wireless computer or the Router, or trying a different channel on the Router.

- Sources of interference: The 2.4Ghz ISM band is used for 802.11b and 802.11g. This is generally a licence free band for low power applications, and you may have other devices at your location that operate in this frequency band. You should take care to ensure that there are no devices like microwave ovens for example close to the Router or wireless computers as this could affect receiver sensitivity and reduce the performance of your network. If you are unsure try relocating both the wireless computers and the Router to establish whether this problem exists.
- Most wireless computer Adapters will scan the channels for the wireless Router. If a wireless computer has not located the Router then try initiating a search manually if the client software supports this feature or manually set the channel on your wireless computer to correspond to the Router channel number. Please refer to your Wireless computer adapter documentation and vendor to do this.
- Speed of connection: The 802.11b and 802.11g standards will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds supported by 802.11g are 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps. The speeds supported by 802.11b are 11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps. In general the closer you are to the Router the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Router or moving the Wireless computer closer to the Router. In an ideal network the Router should be located in the centre of the network with Wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Computer Card documentation and vendor for more details.

Recovering from Corrupted Software

If the system software has become corrupted, the Router will enter a “recovery” state; DHCP is enabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Router unit in this state.

Ensure that one of your computers has a copy of the new software image file stored on its hard disk or available on CD-ROM.

The latest software is available on 3Com's Web site at:

`www.3com.com`

1. Remove power from the Router and disconnect the telephone line and all your computers, except for the one computer with the software image.
2. You will need to reconfigure this computer to obtain an IP address automatically (see "Obtaining an IP Address Automatically" on page 23)
3. Restart the computer, and re-apply power to the Router.
4. Using the Web browser on the computer, enter the following URL in the location bar:

   `http://192.168.1.1`.

   This will connect you to the Recovery utility in the Router.
5. Follow the on-screen instructions. Enter the path and filename of the software image file.
6. When the upload has completed, the Router will restart, run the self-test and, if successful, resume normal operation.
7. Refer to the Installation Guide to reconnect your Router to the telephone line and the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

   If the Router does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.

Frequently Asked Questions

How do I reset the Router to Factory Defaults?

See "Forgotten Password and Reset to Factory Defaults" on page 72.

How many computers on the LAN does the Router support?

A maximum of 253 computers on the LAN are supported.

How many wireless clients does the Router support?

A maximum of 128 wireless clients are supported.

There are only 4 LAN ports on the Router. How are additional computers connected?

You can expand the number of connections available on your LAN by using hubs, switches and wireless access points connected to the Router. 3Com wireless access points and hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

`http://www.3com.com/`

Does the Router support virtual private networks (VPNs)?

The Router supports VPN passthrough, which allows VPN clients on the LAN to communicate with VPN hosts on the Internet. It is also possible to set up VPN hosts on your LAN that clients elsewhere on the Internet can connect to, but this is not a recommended configuration.

Where can I download software updates for the Router?

Updates to the Router software are posted on the 3Com support web site, accessible by visiting:

`http://www.3com.com`

A

IP ADDRESSING

The Internet Protocol Suite

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

Managing the Router over the Network

To manage a device over the network, the Router must be correctly configured with the following IP information:

- An IP address
- A Subnet Mask

IP Addresses and Subnet Masks

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP Address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.

The only value that will be different is the specific host device number. This value must always be unique.

An example IP address is '192.168.100.8'. However, the size of the network determines the structure of this IP Address. In using the Router, you will probably only encounter two types of IP Address and subnet mask structures.

Type One

In a small network, the IP address of '192.168.100.8' is split into two parts:

- Part one ('192.168.100') identifies the network on which the device resides.
- Part two ('.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.255.0'.

See Table 3 for an example about how a network with three computers and a Router might be configured.

Table 3 IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.255.0
PC 2	192.168.100.33	255.255.255.0
PC 3	192.168.100.188	255.255.255.0
Router	192.168.100.72	255.255.255.0

Type Two

In larger networks, where there are more devices, the IP address of '192.168.100.8' is, again, split into two parts but is structured differently:

- Part one ('192.168') identifies the network on which the device resides.
- Part two ('.100.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of ‘255.255.0.0’.

See Table 4 for an example about how a network (only four computers represented) and a Router might be configured.

Table 4 IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.002.230	255.255.0.0
Router	192.168.002.72	255.255.0.0

How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

DHCP Addressing

The Router contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System such as Windows® 95, Windows 98 or Windows NT 4.0. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000.

B TECHNICAL SPECIFICATIONS

This section lists the technical specifications for the OfficeConnect ADSL Wireless 11g Firewall Router.

OfficeConnect ADSL Wireless 11g Firewall Router

Interfaces

DSL connection

LAN connection — four 10Mbps/100Mbps dual speed Ethernet ports (10BASE-T/100BASE-TX)

WLAN Interfaces

Standard IEEE 802.11g, Direct Sequence Spread Spectrum (DSSS)
Transmission rate: 54Mbps, automatic fallback to 48, 36, 24, 18, 12, or 6 Mbps
Maximum channels: 14
Range up to 304.8m (1000ft)
Frequency: (US/Canada/Europe) 2.400-2.4835 GHz
Sensitivity: 6, 12, 18, 24, 36, 48 Mbps: -85 dBm;
54 Mbps -66 dBm typical
Modulation: CCK, BPSK, QPSK, OFDM
Encryption: 40/64 bit WEP, 128 bit WEP, WPA
Maximum clients: 128
O/P Power: 18dBm

Standard IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS)
Transmission rate: 11bps, automatic fallback to 5.5, 2, or 1 Mbps
Maximum channels: 14
Range up to 304.8m (1000ft)
Frequency: (US/Canada/Europe) 2.400-2.4835 GHz
Sensitivity: 1, 2, 5.5 Mbps: -85 dBm; 11 Mbps -82 dBm typical
Modulation: CCK, BPSK, QPSK
Encryption: 40/64 bit WEP, 128 bit WEP, WPA

Maximum clients: 128
O/P Power 16dBm

Operating Temperature

0 °C to 40 °C (32 °F to 105 °F)

Power

8VA, 25 BThU/hr

Humidity

0 % to 90 % (non-condensing) humidity

Dimensions

- Width = 220 mm (8.7 in.)
- Depth = 133 mm (5.2 in.)
- Height = 38 mm (1.5 in.)

Weight

Approximately 550 g (1.1 lbs)

Standards	Functional:	ISO 8802/3 IEEE 802.3 IEEE 802.11b, 802.11g
	Safety:	EN 60950
	EMC:	EN 55022 Class B EN 55024 FCC Part 15 Class B* ETSI EN 301 489–17
	Radio	ETS 300 328 (2.4 GHz ISM band wide band transmission systems.
	Environmental:	EN 60068 (IEC 68)

*See "FCC Statement" on page 105 for conditions of operation.

System Requirements

Operating Systems

The Router will support the following Operating Systems:

- Windows 95/98
- Windows NT 4.0
- Windows ME
- Windows 2000
- Windows XP
- Mac OS 8.5 or higher
- Unix

Ethernet Performance

The Router complies to the IEEE 802.3i, u and x specifications.

Cable Specifications

The Router supports the following cable types and maximum lengths:

- Category 3 (Ethernet) or Category 5 (Fast Ethernet or Dual Speed Ethernet) Twisted Pair — shielded and unshielded cable types.
- Maximum cable length of 100m (327.86 ft).

C

SAFETY INFORMATION

Important Safety Information

WARNING*: Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.*
You must read the following safety information carefully before you install or remove the unit:

WARNING*: The Router generates and uses radio frequency (rf) energy. In some environments, the use of rf energy is not permitted. The user should seek local advice on whether or not rf energy is permitted within the area of intended use.*

WARNING*: Exceptional care must be taken during installation and removal of the unit.*

WARNING*: To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.*

WARNING*: The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.*

WARNING*: This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.*

WARNING*: There are no user-replaceable fuses or user-serviceable parts inside the Router. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.*

WARNING*: Disconnect the power adapter before moving the unit.*

WARNING: RJ-45 ports. *These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.*

Wichtige Sicherheitshinweise

VORSICHT: *Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.*
Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Geräts installieren oder ausbauen:

VORSICHT: *Der Router erzeugt und verwendet Funkfrequenz (RF). In manchen Umgebungen ist die Verwendung von Funkfrequenz nicht gestattet. Erkundigen Sie sich bei den zuständigen Stellen, ob die Verwendung von Funkfrequenz in dem Bereich, in dem der Bluetooth Access Point eingesetzt werden soll, erlaubt ist.*

VORSICHT: *Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.*

VORSICHT: *Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.*

VORSICHT: *Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.*

VORSICHT: *Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.*

VORSICHT: *Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Router haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.*

VORSICHT: *Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.*

VORSICHT: RJ-45-Anschlüsse. *Dies sind abgeschirmte RJ-45-Datenbuchsen. Sie können nicht als Telefonanschlußbuchsen verwendet werden. An diesen Buchsen dürfen nur RJ-45-Datenstecker angeschlossen werden.*

Consignes importantes de sécurité

AVERTISSEMENT: *Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes.*
Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil:

AVERTISSEMENT: *La Router fournit et utilise de l'énergie radioélectrique (radio fréquence -rf). L'utilisation de l'énergie radioélectrique est interdite dans certains environnements. L'utilisateur devra se renseigner sur l'autorisation de cette énergie dans la zone prévue.*

AVERTISSEMENT: *Faites très attention lors de l'installation et de la dépose du groupe.*

AVERTISSEMENT: *Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.*

AVERTISSEMENT: *La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.*

AVERTISSEMENT: *L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 60950. Ces* *conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.*

AVERTISSEMENT: *Il n'y a pas de parties remplaceables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.*

AVERTISSEMENT: *Débranchez l'adaptateur électrique avant de retirer cet appareil.*

AVERTISSEMENT: Ports RJ-45. *Il s'agit de prises femelles blindées de données RJ-45. Vous ne pouvez pas les utiliser comme prise de téléphone. Branchez uniquement des connecteurs de données RJ-45 sur ces prises femelles.*

D END USER SOFTWARE LICENSE AGREEMENT

3Com Corporation
END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION ("3COM") TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE "I AGREE" OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.

LICENSE: 3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the "Software") and accompanying documentation (the "Documentation"), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

ASSIGNMENT; NO REVERSE ENGINEERING: You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union ("EU") resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

EXPORT RESTRICTIONS: The Software, including the Documentation and all related technical data (and any copies thereof) (collectively "Technical Data"), is subject to United States Export control laws and may be subject to export or import regulations in other countries. In addition, the Technical Data covered by this Agreement may contain data encryption code which is unlawful to export or transfer from the United States or country where you legally obtained it without an approved U.S. Department of Commerce export license and appropriate foreign export or import license, as required. You agree that you will not export or re-export the Technical Data (or any copies thereof) or any products utilizing the Technical Data in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, re-export or import the Technical Data.

In addition to the above, the Product may not be used, exported or re-exported (i) into or to a national or resident of any country to which the U.S. has embargoed; or (ii) to any one on the U.S. Commerce Department's Table of Denial Orders or the U.S. Treasury Department's list of Specially Designated Nationals.

TRADE SECRETS; TITLE: You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

UNITED STATES GOVERNMENT LEGENDS: The Software, Documentation and any other technical data provided hereunder is commercial in nature and developed solely at private expense. The Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

TERM AND TERMINATION: The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

LIMITED WARRANTIES AND LIMITATION OF LIABILITY: All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software. Such warranties and limitations of liability are incorporated herein in their entirety by this reference.

GOVERNING LAW: This Agreement shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

SEVERABILITY: In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

ENTIRE AGREEMENT: This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

3Com Corporation, 350 Campus Drive, Marlborough, MA. USA 01752-3064

D OBTAINING SUPPORT FOR YOUR PRODUCT

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at `http://eSupport.3com.com/`. 3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request.

Purchase Value-Added Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com Extended Warranty and Professional Services is available at `http://www.3com.com/`

Contact your authorized 3Com reseller or 3Com for additional product and support information.

Troubleshoot Online

You will find support tools posted on the 3Com web site at `http://www.3com.com/`

- **3Com Knowledgebase** helps you troubleshoot 3Com products. This query-based interactive tool is located at `http://knowledgebase.3com.com` and contains thousands of technical solutions written by 3Com support engineers.
- **Connection Assistant** helps you install, configure and troubleshoot 3Com desktop and server NICs, wireless cards and Bluetooth devices. This diagnostic software is located at:

http://www.3com.com/prodforms/software/connection_assistant/ca_thankyou.html

Access Software Downloads

Software Updates are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com web site at **http://eSupport.3com.com/**.

First time users will need to apply for a user name and password. A link to software downloads can be found at **http://eSupport.3com.com/**, or under the Product Support heading at **http://www.3com.com/**

Software Upgrades are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Contact Us

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address from the list below. You will find a current directory of support telephone numbers posted on the 3Com web site at **http://csoweb4.3com.com/contactus/**

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at **http://eSupport.3com.com/**

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at `http://eSupport.3com.com/`. First time users will need to apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of support telephone numbers posted on the 3Com web site at `http://csoweb4.3com.com/contactus/`

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim Telephone Technical Support and Repair			
Australia	1 800 678 515	Philippines	1235 61 266 2602 or
Hong Kong	800 933 486		1800 1 888 9469
India	+61 2 9424 5179 or	P.R. of China	10800 61 00137 or
	000800 650 1111		021 6350 1590 or
Indonesia	001 803 61009		00800 0638 3266
Japan	00531 616 439 or	Singapore	800 6161 463
	03 5977 7991	S. Korea	080 333 3308
Malaysia	1800 801 777	Taiwan	00801 611 261
New Zealand	0800 446 398	Thailand	001 800 611 2000
Pakistan	+61 2 9937 5083		
You can also obtain support in this region using the following e-mail: `apr_technical_support@3com.com`			
Or request a repair authorization number (RMA) by fax using this number:			+ 65 543 6348
Europe, Middle East, and Africa Telephone Technical Support and Repair			
From anywhere in these regions, call:	+44 (0)1442 435529		
From the following countries, you may use the numbers shown:			
Austria	01 7956 7124	Luxembourg	342 0808128
Belgium	070 700 770	Netherlands	0900 777 7737
Denmark	7010 7289	Norway	815 33 047
Finland	01080 2783	Poland	00800 441 1357
France	0825 809 622	Portugal	707 200 123
Germany	01805 404 747	South Africa	0800 995 014
Hungary	06800 12813	Spain	9 021 60455
Ireland	01407 3387	Sweden	07711 14453
Israel	1800 945 3794	Switzerland	08488 50112
Italy	199 161346	U.K.	0870 909 3266

You can also obtain support in this region using the following URL:
`http://emea.3com.com/support/email.html`

Country	Telephone Number	Country	Telephone Number
Latin America Telephone Technical Support and Repair			
Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

You can also obtain support in this region using the following:

Spanish speakers, enter the URL:
`http://lat.3com.com/lat/support/form.html`

Portuguese speakers, enter the URL:
`http://lat.3com.com/br/support/form.html`

English speakers in Latin America should send e-mail to:
`lat_support_anc@3com.com`

US and Canada Telephone Technical Support and Repair			
	1 800 876 3266		

Published 16th July 2003

GLOSSARY

802.11b	The IEEE specification for wireless Ethernet which allows speeds of up to 11 Mbps. The standard provides for 1, 2, 5.5 and 11 Mbps data rates. The rates will switch automatically depending on range and environment.
802.11g	The IEEE specification for wireless Ethernet which allows speeds of up to 54 Mbps. The standard provides for 6, 12, 24, 36, 48 and 54 Mbps data rates. The rates will switch automatically depending on range and environment.
10BASE-T	The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.
100BASE-TX	The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.
Access Point	An Access Point is a device through which wireless clients connect to other wireless clients and which acts as a bridge between wireless clients and a wired network, such as Ethernet. Wireless clients can be moved anywhere within the coverage area of the access point and still connect with each other. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless client radio traffic and forwarding wireless client messages to the Ethernet LAN.
Ad Hoc mode	Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infrastructure mode, which is the mode the router uses. (see also Infrastructure mode.)
Auto-negotiation	Some devices in the range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best

common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

Bandwidth The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. The bandwidth for 802.11b wireless is 11Mbps.

Category 3 Cables One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 3 is voice grade cable and can only be used in Ethernet networks (10BASE-T) to transmit data at speeds of up to 10 Mbps.

Category 5 Cables One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

Channel Similar to any radio device, the Wireless Cable/DSL router allows you to choose different radio channels in the wireless spectrum. A channel is a particular frequency within the 2.4GHz spectrum within which the Router operates.

Client The term used to described the desktop PC that is connected to your network.

DHCP Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

DNS Server Address DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing “3com.com” into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL modem	DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.
Encryption	A method for providing a level of security to wireless data transmissions. The Router uses two levels of encryption; 40/64 bit and 128 bit. 128 bit is a more powerful level of encryption than 40/64 bit.
ESSID	Extended Service Set Identifier. The ESSID is a unique identifier for your wireless network. You must have the same ESSID entered into the router and each of it's wireless clients.
Ethernet	A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.
Ethernet Address	See MAC address.
Fast Ethernet	An Ethernet system that is designed to operate at 100 Mbps.
Firewall	Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.
Full Duplex	A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.
Half Duplex	A system that allows packets to transmitted and received, but not at the same time. Contrast with full duplex.
Hub	A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.

IEEE	Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.
IETF	Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.
Infrastructure mode	Infrastructure mode is the wireless configuration supported by the Router. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Router. (see also Ad Hoc mode)
IP	Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.
IP Address	Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.
ISP	Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.
LAN	Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).
MAC	Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC Address	Media Access Control Address. Also called the hardware or physical address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.
NAT	Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Router allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.
Network	A Network is a collection of computers and other computer equipment that are connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.
Network Interface Card (NIC)	A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.
Protocol	A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.
PPPoE	Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.
PPTP	Point-to-Point Tunneling Protocol is a method of secure data transmission between two remote sites over the internet.
RJ-45	A standard connector used to connect Ethernet networks. The “RJ” stands for “registered jack”.
Router	A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.

Server	A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.
SSID	Service Set Identifier. Some vendors of wireless products use SSID interchangeably with ESSID.
Subnet Address	An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.
Subnet mask	A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).
Subnets	A network that is a component of a larger network.
Switch	A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.
TCP/IP	Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet. TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.
Traffic	The movement of data packets on a network.
universal plug and play	Universal plug and play is a system which allows compatible applications to read some of their settings from the Router. This allows them to automatically configure some, or all, of their settings and need less user configuration.

URL Filter	A URL Filter is a feature of a firewall that allows it to stop its clients form browsing inappropriate Web sites.
WAN	Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.
WECA	Wireless Ethernet Compatibility Alliance. An industry group formed to certify cross vendor interoperability and compatibility of 802.11b and 802.11g wireless networking products and to promote the standard for enterprise, small business and home environments. (see also 802.11b, 802.11g, Wi-Fi)
WEP	Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.
Wi-Fi	Wireless Fidelity. This is the certification granted by WECA to products that meet their interoperability criteria. (see also 802.11b, WECA)
Wireless Client	The term used to describe a desktop or mobile PC that is wirelessly connected to your wireless network
Wireless LAN Service Area	Another term for ESSID (Extended Service Set Identifier)
Wizard	A Windows application that automates a procedure such as installation or configuration.
WLAN	Wireless Local Area Network. A WLAN is a group of computers and devices connected together by wireless in a relatively small area (such as a house or office).
WPA	Wi-Fi Protected Access. A dynamically changing encryption mechanism for wireless networking. Encryption strength is 256 bit.

INDEX

A

Addresses
  IP 77
Automatic Addressing 79

C

Cable Specifications 83
Channels 105
Conventions
  notice icons, About This Guide 8
  text, About This Guide 8

D

DHCP 38, 79
DHCP Server 25
DNS 24
Dynamic IP Address 31

F

Forgotten Password 72

I

Internet
  addresses 77
IP Address 37, 77

L

LED 14

N

Network
  addresses 77
Networking
  wireless 73
NIC
  wireless 14

P

Password 27
PPPoE 26, 30, 31

R

Reset to Factory Defaults 72

S

Safety Information 17
Setup Wizard 27
Specifications
  technical 81
Static Addressing 79
Subnet Mask 77
Summary 33

T

TCP/IP 23, 25, 77
Technical
  specifications 81
  standards 81

W

Web Proxy 26
Wireless
  LED 15
  networking 73
  NIC 14

REGULATORY NOTICES FOR THE OFFICECONNECT ADSL WIRELESS 11G FIREWALL ROUTER

Channels

Use of the OfficeConnect ADSL Wireless 11g Firewall Router is only authorized for the channels approved by each country. For proper installation, login to the management interface and select your country from the drop down list. Table 5 below details the channels permitted by the local regulatory agencies:

Table 5 Channels

Channels	Country
1 - 13	Australia, Austria, Bahrain, Belarus, Belgium, Chile, China, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Finland, France*, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Liechtenstein, Lithuania, Luxembourg, Malaysia, Netherlands, New Zealand, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Russia, Saudi Arabia, Singapore, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Turkey, United Kingdom, Uruguay, Venezuela.
1 - 11	Argentina, Brazil, Canada, Columbia, Mexico, Taiwan, United States
10 - 13	France*, Jordan
1-14	Japan

* The channels available for use in France depend on the region in which you are located.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, “Digital Apparatus,” ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation.

Information to the User

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.
- Consult the dealer or an experienced radio/television technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4. In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

FCC Declaration of Conformity

We declare under our sole responsibility that the

Model:	**Description:**
3CRWE754G72-A/B	OfficeConnect ADSL Wireless 11g Firewall Router

to which this declaration relates, is in conformity with the following standards or other normative documents:

- ANSI C63.4-1992 Methods of Measurement
- Federal Communications Commission 47 CFR Part 15, subpart B
  15.107 (a)Class B Conducted Limits
  15.109 (a)Class B Radiated Emissions Limits

- 15.107 (e)Class B Conducted Limits
  15.109 (g)Class B Radiated Emissions Limits

Exposure to Radio Frequency Radiation: The radiated output power of the 3Com ADSL 11g Wireless Router is far below the FCC radio frequency exposure limits. Nevertheless, the 3Com OfficeConnect ADSL Wireless 11g Firewall Router shall be used in such manner that the potential for human contact during normal operation is minimized. The distance between the antennas and the user should not be less than 20 cm.

CE Statement (Europe)

This product complies with the European Low Voltage Directive 73/23/EEC, EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC and the Radio and Telecommunications Terminal Equipment Directive 99/5/EC.

FCC

⚠ ***CAUTION:*** *To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.*

RF Exposure Compliance Statement (U.S.)

⚠ ***CAUTION****: The 3Com OfficeConnect ADSL Wireless 11g Firewall Router has been certified as a mobile computing device as per FCC Section 2.1091. In order to comply with the FCC RF exposure requirements, the 3Com ADSL 11g Wireless Router must only be installed with approved antennas and a minimum separation distance of 20 cm (8 in) must be maintained from the antenna to any nearby persons.*

3Com Corporation, Corporate Headquarters,

350 Campus Drive, Marlborough, MA
USA 01752-3064

To learn more about 3Com products and services,
visit our World Wide Web site at **www.3com.com**

All specifications are subject to change without notice.

Copyright © 2004 3Com Corporation. All rights reserved.
3Com and are registered trademarks of 3Com
Corporation. All other company and product names may
be trademarks of their respective companies.

DUA0075-4AAA01
Rev. 01